EXHIBIT 1

[REDACTED COPY]

United States v. Zeitlin,
23 Cr. 419 (LAK)

THE GOVERNMENT'S OMNIBUS MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S PRETRIAL MOTIONS TO DISMISS THE INDICTMENT, FOR A BILL OF PARTICULARS, AND TO SUPPRESS EVIDENCE SEIZED FROM CERTAIN PREMISES

Filed: December 14, 2023

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Twenty-Nine Electronic Devices Seized in Las Vegas, Nevada, on or about August 17, 2023, USAO No. 2018R01129

23 MAG 6429

Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attached Affidavit and its Attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1343, 1349, 2326, 2	Wire fraud and conspiracy to commit wire fraud
18 U.S.C. 1512(c), (k), 2	Obstruction of justice and conspiracy to commit obstruction of justice

The application is based on these facts:

Please see Attached Affidavit and its Attachment A.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Kelsey Palermo (By Court with Authorization)
Applicant's signature

Kelsey Palermo, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime *(specify reliable electronic means).*

Date: 09/15/2023

Judge's signature

City and state: New York, New York

The Hon. Sarah L. Cave, U.S.M.J.
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

23 MAG 6429

In the Matter of the Application of the United States of America for a Search and Seizure Warrant for Twenty-Nine Electronic Devices Seized in Las Vegas, Nevada, on or about August 17, 2023, USAO No. 2018R01129

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

KELSEY PALERMO, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI for approximately eight years, and for three years before that I worked as a Staff Operations Specialist with the FBI. For approximately two years, I have been assigned to a public corruption squad in the FBI's New York field office. Prior to the FBI's public corruption squad, I was assigned to an FBI counter-intelligence squad. As an FBI Special Agent, I have participated in numerous investigations involving public corruption offenses and fraud, including telemarketing fraud and wire fraud offenses. I have also participated in the execution of search warrants involving premises and electronic evidence. Through my training, education, and experience, I am familiar with the techniques and methods of operation commonly used by individuals engaged in fraud to communicate, operate their scheme(s), conceal their criminal activities, and avoid detection by law enforcement. I am also familiar with the means and methods commonly used by individuals who obstruct justice, including by destroying or deleting evidence and/or directing others to destroy or

delete evidence. As an FBI Special Agent, I have received training in the enforcement of federal laws pertaining to public corruption and fraud offenses, including: (1) debriefing defendants, witnesses, and informants, as well as others who have knowledge of public corruption offenses, obstruction offenses, and schemes to defraud, including wire fraud, telemarketing fraud, and frauds that involve political action committees ("PACs"); (2) the planning, participation, and/or management of field operations such as surveillance, arrests, the interception of wire communications, and the execution of search warrants; (3) the acquisition, preservation, processing, and analysis of evidence; (4) the seizure, search, and analysis of electronic devices and electronically stored information; and (5) the tracking of crime proceeds.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. Each of the Subject Devices were seized in Las Vegas, Nevada, by the FBI on or about August 17, 2023, pursuant to judicially authorized search and seizure warrants. Specifically, as set forth below, the Subject Devices were seized from two properties associated with Richard

Zeitlin: (a) Zeitlin's residence at 7815 West La Madre Way, Las Vegas Nevada 89149 ("Zeitlin Premises-1"); and (b) a business property used and at least partially owned by Zeitlin at 1835 East Charleston Boulevard, Las Vegas, Nevada 89104 ("Zeitlin Premises-2," and together with Zeitlin Premises-1, the "Zeitlin Premises"). The Subject Devices are particularly described as follows:

Subject Device	Description	FBI Item No. [1]	Seizure Premises
1	Grey Apple iPad tablet with black keyboard case, Model A2378, S/N T045J4W21D	1B17	Zeitlin Premises-1
2	Apple iMac computer, Model A1419, S/N C02X61YWJ1GH	1B18	Zeitlin Premises-1
3	Apple iPad tablet, Model A1822, S/N DMPZKKJJHLF9	1B23	Zeitlin Premises-1
4	Samsung Galaxy Note 9 cellphone, Model SM-N6904, IMEI 351884708468626	1B25	Zeitlin Premises-1
5	White and gold Apple iPhone cellphone, IMEI 351884708468626	1B26	Zeitlin Premises-1
6	Apple iPad tablet, Model A1822, S/N DMPVKJTAHLF9	1B32	Zeitlin Premises-1
7	Samsung cellphone, Model SM-S908VZWFXAA, IMEI 357111203204742	1B34	Zeitlin Premises-1
8	Apple iPhone cellphone, Model A2651, S/N CXRTWW4P6K	1B35	Zeitlin Premises-1
9	Apple MacBook Pro laptop computer, Model A1502, S/N C02RG06DFVH9	1B36	Zeitlin Premises-1
10	Apple iMac computer, Model A2115, S/N H12DFHJLPN77	1B39	Zeitlin Premises-1
11	Grey Apple MacBook Pro, Model A2141, S/N C02FC6H1M-D6N	1B16	Zeitlin Premises-1
12	Silver Samsung cellphone with case, IMEI 351381563505451[2]	1B15	Zeitlin Premises-1
13	Desktop Computer, Service Tag D33DHX1	1B46	Zeitlin Premises-2
14	Desktop Computer, Service Tag D36DHX1	1B47	Zeitlin Premises-2
15	Desktop Computer, Service Tag D2XCHX1	1B48	Zeitlin Premises-2
16	Dell Chromebook Computer, Serial Tag 6DNZ28B2	1B49	Zeitlin Premises-2

[1] The FBI assigns item numbers to certain physical items seized as part of a particular investigation. Each of the item numbers referenced herein pertains to the item number within the FBI file for this particular investigation.

[2] Based on my training and experience, I know that an "IMEI" number is a unique identifier assigned to certain cellphone devices.

Subject Device	Description	FBI Item No. [1]	Seizure Premises
17	Desktop Tower with Post-It Note and "ENERMAX" case	1B50	Zeitlin Premises-2
18	Desktop Computer, Service Tag D33BHX1	1B51	Zeitlin Premises-2
19	Desktop Computer, Service Tag D30CHX1	1B52	Zeitlin Premises-2
20	Desktop Computer, Service Tag D34DHX1	1B53	Zeitlin Premises-2
21	Desktop Computer GGPPK02	1B54	Zeitlin Premises-2
22	Hard Drive	1B74	Zeitlin Premises-2
23	Hard Drive, S/N WX20C7979315	1B75	Zeitlin Premises-2
24	Kensington USB Drive 17009	1B78	Zeitlin Premises-2
25	Phone with call number 702-278-1275	1B79	Zeitlin Premises-2
26	SanDisk USB drive	1B80	Zeitlin Premises-2
27	Hard Drive, S/N 11500325584F	1B81	Zeitlin Premises-2
28	Desktop Computer, Service Tag D35DHX1	1B88	Zeitlin Premises-2
29	Dell Optiplex 3010 Desktop Computer, Service Tag D2ZDHX1	1B87	Zeitlin Premises-2

4. Based on my training, experience, and research, I know that the Subject Devices are cellphones and tablet computers have capabilities that allow them to each serve as a wireless telephone, digital camera, portable media player, GPS navigation device, text and multimedia message device, and PDA including access to the internet. I know that the Subject Devices that are desktop and laptop computers have capabilities that allow them to each serve as electronic communication devices, store financial and other electronic records, and access the internet. The Subject Devices that are USB drives or hard drives have capabilities that allow them to store any type of electronic records, including communications and financial records.

5. The Subject Devices are presently located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I submit that there is probable cause to believe that the Subject Devices contains evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1349 and 2326 (conspiracy to commit wire fraud); 18 U.S.C. §§ 1343, 2326, and 2 (wire fraud);

18 U.S.C. § 1512(c), (k) (conspiracy to obstruct justice); and 18 U.S.C. §§ 1512(c) and 2 (obstruction of justice) (the "Subject Offenses").

II. Probable Cause

7. Richard Zeitlin, the defendant, has been charged in Indictment No. 23 Cr. 419 (LAK) (the "Indictment") with: (1) conspiracy to commit wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1349 and 2326; (2) wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1343, 2326, and 2; (3) conspiracy to obstruct justice in or about May 2022, in violation of 18 U.S.C. § 1512(c), (k); and (4) obstruction of justice in or about May 2022, in violation of 18 U.S.C. §§ 1512(c) and 2. The Indictment is attached hereto as Exhibit A and incorporated as if fully set forth herein.

8. On or about August 16, 2023, the Honorable Cam Ferenbach, United States Magistrate Judge, District of Nevada, issued warrants (the "Prior Warrants") to (1) search (a) Zeitlin's residence at 7815 West La Madre Way, Las Vegas Nevada 89149, *i.e.*, Zeitlin Premises-1; and (b) a business property used and at least partially owned by Zeitlin at 1835 East Charleston Boulevard, Las Vegas, Nevada 89104, *i.e.*, Zeitlin Premises-2; and (2) seize evidence, fruits, and instrumentalities of the Subject Offenses from the Zeitlin Premises, including electronic devices, as set forth in the Prior Warrants. The Prior Warrants and the applications submitted in support of the Prior Warrants (the "Prior Applications") are attached hereto as Exhibit B and incorporated as if fully set forth herein.[3] In the Prior Applications, and consistent with the practices in the District of Nevada, the Government indicated that it would transport any electronic devices seized from

[3] Each of the Prior Applications includes the same agent affidavit. For purposes of completeness, Exhibit A includes each of the Prior Applications, despite the duplication of the agent affidavit, and each of the Prior Warrants. Citations to paragraphs of the Prior Applications, accordingly, refer to the same paragraphs within each of the Prior Applications.

the Zeitlin Premises to the Southern District of New York and obtain a second warrant in this District to search the electronic devices for evidence, fruits, and instrumentalities of the Subject Offenses.

9. Based on my participation in this investigation, my conversations with other law enforcement officers, and my review of documents and reports relating to the execution of the Prior Warrants, I know that on or about August 17, 2023, law enforcement officers executed the Prior Warrants and seized the Subject Devices from the Zeitlin Premises. Specifically, Subject Devices-1 through -12 were seized from Zeitlin Premises-1 and Subject Devices-13 through -29 were seized from Zeitlin Premises-2.

10. The Prior Applications set forth probable cause to seize the Subject Devices from Zeitlin Premises-1, Zeitlin's home in Las Vegas, because they are likely to contain evidence, fruits, and instrumentalities of the Subject Offenses. *See* Prior Applications ¶¶ 7-29. In addition, based on the Prior Applications and the following, I believe that there is probable cause that the Subject Devices seized from Zeitlin Premises-1 were used by Zeitlin and are likely to contain evidence, fruits, and instrumentalities of the Subject Offenses.[4] Among other things, Zeitlin utilized electronic communications to carry out the Subject Offenses, namely his fraud and his obstruction of justice schemes. For example, since at least in or about 2018, Zeitlin has maintained a practice of communicating with his employees principally through phone or encrypted messaging applications. Indictment ¶ 14; Prior Applications ¶¶ 12(g), 19. Likewise, Zeitlin employees worked remotely, so they necessarily communicated with the owner of that business, Zeitlin, using electronic devices. Prior Applications ¶ 19. Based on my involvement in this investigation, I know

[4] To the extent that law enforcement officers determine that any of the Subject Devices were not used by Zeitlin, they will cease search of the device and will make best efforts to return the device to its owner and/or user (if that owner and/or user is identifiable).

that Zeitlin employees frequently used Skype to communicate with one another about the operations of the call centers. Indictment ¶ 15. In or about May 2022, Zeitlin instructed one particular associate, CC-1, to tell his employees to delete their Skype messages after he learned about grand jury subpoenas. *Id.* CC-1 relayed that instruction to at least one Zeitlin employee using Signal, an encrypted messaging application. Prior Applications ¶ 19 n.6. Zeitlin's online activity suggested that he had banking activity at different financial institutions, and his electronic devices may show evidence of his banking activity at those institutions. Prior Applications ¶ 21.

11. Although Zeitlin's fraud scheme ran from in or about 2017 through at least in or about 2020, *see* Indictment ¶¶ 17, 20, his obstruction occurred in or about May 2022 and he had online activity related to potential criminal charges, FEC compliance, and banking activity as recently as March 2023 and April 2023. Prior Applications ¶ 21. Moreover, based on my training and experience, given the nature of Zeitlin's business and his supervision over a sprawling call center business, among other things, I believe key records regarding his call center business include electronic records stored on electronic devices, including those found in his home and businesses. *See id.* ¶¶ 10-14.

Zeitlin Premises-1

Subject Devices Seized from the Casita of Zeitlin Premises-1

12. Based on my review of documents and records pertaining to the execution of the Prior Warrants, my participation in this investigation, and my conversations with other law enforcement officers, I know that as of on or about August 17, 2023, Zeitlin lived at Zeitlin Premises-1 with his spouse ("Individual-1"), from whom he is in the process of divorcing. Zeitlin has two adult children, both of whom reside in Wisconsin (*i.e.* not at Zeitlin Premises-1). I am not

aware of any other individuals other than Zeitlin and Individual-1 who resided at Zeitlin Premises-1 on or about August 17, 2023.

13. Based on my conversations with other law enforcement officers who spoke with Individual-1 on or about August 17, 2023, my participation in this investigation, and my review of documents and records pertaining to the execution of the Prior Warrants, I know that as of on or about August 17, 2023, Individual-1 was using a casita (the "Casita") at Zeitlin Premises-1, a structure similar to a pool house, in-law suite, or guest suite, as her sleeping quarters, and Zeitlin was using the master bedroom in the main structure at Zeitlin Premises-1 as his sleeping quarters. While law enforcement officers were searching Zeitlin Premises-1, Individual-1 stated that two cellphones belonged to her. Individual-1 identified the two devices that belonged to her, and Individual-1 took one of those devices with her and left Zeitlin Premises-1. Individual-1 did not claim ownership of the remaining electronic devices at Zeitlin Premises-1, including from inside the Casita (nor did she specifically identify the user(s) of the electronic devices at Zeitlin Premises-1 other than the ones she claimed). Neither of the two devices Individual-1 identified as belonging to her is included among the Subject Devices.

14. Based on my review of documents and records pertaining to the execution of the Prior Warrants, I know that Subject Devices-7, -8, -9, and -10 were seized from the Casita. Specifically, within the Casita, Subject Devices-7 and -8 were seized from a mesh pouch in a cabinet under the television in the bedroom of the Casita; Subject Device-9 was seized from the bottom right hand door of a cabinet under the television in the bedroom of the Casita; and Subject Device-10 was seized from on top of the sink counter in the bathroom of the Casita.

15. Based on my participation in this investigation, including my conversations with other law enforcement officers, I know Zeitlin Premises-1 has a pool and that casitas like the Casita

often have various functions, and are often used as, for example, pool houses, home offices, in-law suites, and/or bedrooms. I also know that individuals who reside in homes and/or larger properties often store and/or place their belongings through the property, regardless of where they sleep. Based on my training and experience, I believe that the fact that Individual-1 did not identify Subject Devices-7 through -10 as belonging to her, combined with the fact that they were located within the premises where Zeitlin lived, shows that Zeitlin was likely a user of these Subject Devices. Furthermore, based on my training and experience, even if Zeitlin was only one of multiple users of these Subject Devices, those devices may be "synced" to online accounts that Zeitlin used in furtherance of the fraud, and may contain relevant electronic records for that reason too. *See* Prior Applications ¶¶ 12(g), 13.

Subject Devices Seized from the Master Bedroom of Zeitlin Premises-1

16. Based on my review of documents and records pertaining to the execution of the Prior Warrants, my participation in this investigation, and my conversations with other law enforcement officers, I know that Subject Devices-3, -4, -5, and -12, were seized from the master bedroom of Zeitlin Premises-1. Specifically, within the master bedroom at Zeitlin Premises-1: Subject Device-3 was seized from the top of a speaker; Subject Device-4 was seized from a safe inside a closet to the master bedroom; Subject Device-5 was seized from inside a suitcase on top of a chair inside a closet to the master bedroom; and Subject Device-12 was seized from on top of the nightstand in the master bedroom.

17. As set forth above, I know that Individual-1 identified certain devices from the Casita that belonged to her and did not claim ownership of Subject Devices-3, -4, -5, and -12.

18. Based on my training and experience, I know that individuals typically place their personal cellphones within their bedrooms; primary cellphones close to or in the vicinity of their

beds when they go to sleep (*e.g.*, on the nightstand); cellphones that contain information and/or data that they may wish to preserve or that may be important in storage areas within a home (*e.g.*, in closets); and cellphones containing important and/or confidential information within locked containers such as safes.

Subject Devices Seized from the Home Office of Zeitlin Premises-1

19. As set forth in the Prior Applications, inside Zeitlin Premises-1, Zeitlin maintains a home office (the "Home Office") and documents obtained during the course of this investigation include a photograph of the defendant seated at a large wooden desk (the "Desk") in the Home Office that matches a photograph of the Desk in the Home Office publicly available on Zillow.com. Prior Applications ¶ 20 & n.8.

20. Based on my review of documents and records pertaining to the execution of the Prior Warrants, my participation in this investigation, and my conversations with other law enforcement officers, I know that Subject Devices-1, -2, and -11 were seized from the top of the Desk within the Home Office.

Subject Devices Seized from the Kitchen of Zeitlin Premises-1

21. Based on my review of documents and records pertaining to the execution of the Prior Warrants, my participation in this investigation, and my conversations with other law enforcement officers, I know that Subject Device-6 was seized from on top of a counter in the kitchen of Zeitlin Premises-1.

22. Based on my review of law enforcement records and my conversations with other law enforcement officers, I know that law enforcement officers found and seized items other than the Subject Devices from Zeitlin Premises-1 that constitute evidence, fruits, and/or instrumentalities of the Subject Offense. For example, law enforcement officers seized from the

Home Office physical documents labeled in search invoice records as call center documents and Federal Election Commission documents.

Subject Devices Seized from Zeitlin Premises-2

23. As set forth in the Prior Applications, until in or about 2018, two entities associated with the Zeitlin call centers were headquartered at Zeitlin Premises-2. *Id.* ¶ 23(a)(ii). Since in or about 2020, a company that Zeitlin partially owns, Chrome Builders Construction, formally operated out of Zeitlin Premises-2. *Id.* However, based on electronic communications and interviews with witnesses, I have learned that, as of in or about July 2023, Zeitlin Premises-2 continues to be occupied by an employee working for the Zeitlin call centers. *Id.* ¶¶ 23(c)-(d). The call center work done at Zeitlin Premises-2 has included scripting, which is a function central to the Subject Offenses. *Id.*; Indictment ¶¶ 7-13. [redacted]

24. Based on my involvement in the search of Zeitlin Premises-2 and my communication with other law enforcement officers, I have learned that when officers executed a search of Zeitlin Premises-2, they learned from Zeitlin that an employee of Zeitlin's who provides

services to Zeitlin's call center business (referred to as "Employee-2" in the Prior Applications) knew the security code for Subject Premises-2. The Government called the attorney for Employee-2, who provided the security code to Subject Premises-2. While searching Zeitlin Premises-2, law enforcement found three primary areas inside the premises: (1) a large room upon entry into the premises (the "Main Room"); (2) a room to the left of the main room that appeared to be used for storage (the "Storage Room"); and (3) a room towards the back of the premises that was suitable for an small office or storage room (the "Office Room").

25. Based on my review of law enforcement records and my involvement in the search of Zeitlin Premises-2, I have learned that law enforcement officers seized Subject Devices-13 through -29 from Zeitlin Premises-2 pursuant to the Prior Warrants. Specifically, the following devices were seized from the three rooms in Zeitlin Premises-2:

a. Storage Room: Subject Devices-13 through -16 were seized from inside a box on the floor of the Storage Room; Subject Device-17 was seized from the floor area across from a desk in the Storage Room; and Subject Device-20 was seized from on top of a desk in the Storage Room.

b. Main Room: Subject Devices-18 and -19 were seized from a desk in the rear part of the Main Room; Subject Device-28 was seized from under the front desk in the Main Room; and Subject Device-29 was seized from on a cabinet counter in the Main Room. There is a Post-It note attached to Subject Device-29 with handwriting that says "recording station" and "6-2-2021."[5]

[5] Based on my review of FBI records for the search of Zeitlin Premises-2, I know that Subject Device-29 is listed in search invoice records as "Dell Computer Modem Service tag D2ZDHX1." However, based on my personal observation of Subject Device-29 in FBI custody, I believe it is a desktop computer, as set forth herein, and not a computer modem.

c. Office Room: Subject Device-21 was seized from on top of a desk in the Office Room; and Subject Devices-22 through -27 were seized from inside a cardboard box located behind a chair and next to the trash in the Office Room. Subject Devices-25 and -26 were further located inside a lock box within the cardboard box.

26. Based on my review of law enforcement records, I have learned that, in addition to the aforementioned Subject Devices, law enforcement officers also recovered from Zeitlin Premises-2 physical documents and records relevant to the Subject Offenses, including but not limited to printed call script records; mail sorted into sets for different business entities that operated the Zeitlin call centers, such as Advanced Telephony Consultants and Wired4Data; mail addressed to TPFE, another business entity that operated the Zeitlin call centers; and financial records belonging to different business entities that operated the Zeitlin call centers.

27. Based on my training and experience and my conversations with other law enforcement officers and my participation in this investigation, including my participation in interviews of [redacted], I know that telemarketing work, including work relating to call centers, typically involves the regular use of electronic devices, such as computers—unlike construction or contracting work. I also know that office spaces that include many electronic devices, including storage devices, hard drives, and computers, indicate that the business that occupied the space used numerous electronic devices and electronic storage devices.

28. Based on my experience and training, I know that spaces like the Storage Room are where businesses typically store files, records, electronics, data, and old furniture and equipment that may not need to be immediately accessed, electronic devices that have been upgrade, and/or electronic devices that were used by employees who are no longer working for the business. For example, the Subject Devices found in the Storage Room are likely to be computers and other

electronic devices that have been upgraded and/or that are no longer actively used by employees of Zeitlin's businesses.

29. Based on my experience and training, I know that office spaces like the Office Room are more private than the Main Room, and are typically where individuals who use the office space store files, records, electronics, and data. For example, based on my participations in this investigation, I believe that the Office Room may have been the office that Employee-3 used when working at Zeitlin Premises-2.

* * *

30. Like individuals engaged in any other kind of activity, individuals who manage large-scale businesses, such as the Zeitlin call centers, and also engage in illegal activity, like the defendant, store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Subject Devices. Such records can include, for example, *e.g.*, "logs of online "chats" with co-conspirators;" "email correspondence;" "contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts;" "stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals;" and/or "records of illegal transactions using stolen financial and personal identification data." Individuals engaged in criminal activity often store such records in order to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (4) store stolen data for future exploitation. *See generally* Prior Applications ¶¶ 10-14 (describing common work and communication practices).

31. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Device. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve from information from the Subject Device depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.]

32. In addition to probable cause to believe that the Subject Device contains evidence and fruits of the Subject Offenses, there is also probable cause to believe that the Subject Devices also constitute instrumentalities of the Subject Offenses, *e.g.*, they were used in furtherance of the Subject Offenses.

33. Based on the foregoing, I respectfully submit there is probable cause to believe that Zeitlin was engaged in the Subject Offenses, and that evidence and fruits of this criminal activity is likely to be found on the Subject Devices.

III. Procedures for Searching ESI

A. Review of ESI

34. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

35. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);

- "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

36. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Devices

37. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

38. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

/s Kelsey Palermo (By Court with Authorization)
_____
KELSEY PALERMO
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means (FaceTime),
pursuant to Federal Rules of Criminal Procedure 41(d)(3)
and 4.1, this 15th day of September, 2023

_____
HON. SARAH L. CAVE
UNITED STATES MAGISTRATE JUDGE

Exhibit A

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

RICHARD ZEITLIN,

Defendant.

SEALED INDICTMENT

23 Cr. _____ (___)

23 CRIM 419

The Grand Jury charges:

OVERVIEW

1. RICHARD ZEITLIN, the defendant, has controlled and operated telemarketing call centers (the "Zeitlin Call Centers") for decades, including from at least in or about 1994 to in or about 2023. The Zeitlin Call Centers have raised at least approximately hundreds of millions of dollars for charities and political action committees ("PACs") through at least approximately hundreds of thousands of calls to donors and potential donors and various entities that ZEITLIN controlled (the "Zeitlin Entities"). From at least in or about 2017 through at least in or about 2020, ZEITLIN used the Zeitlin Call Centers to defraud numerous donors and potential donors by providing misleading and false information about how the donors' money would be spent and the nature of the organizations to which they were giving. For example, ZEITLIN directed his employees to make calls on behalf of certain PACs that falsely portrayed the PAC as a charity and/or a direct-services organization rather than as a PAC. Even after receiving complaints that the Zeitlin Call Centers were providing false and misleading information to donors and potential donors during fundraising calls, ZEITLIN continued his fraudulent scheme and made efforts to conceal it. The Zeitlin Entities profited from ZEITLIN's fraud, typically keeping a large portion

of each dollar donated—approximately 90 percent—the rest of which was disbursed to the respective PAC.

2. In or about May 2022, after learning that he and the Zeitlin Entities were under federal investigation, RICHARD ZEITLIN, the defendant, directed at least one of his employees ("CC-1") to instruct other employees of the Zeitlin Entities to delete electronic messages relating to the Zeitlin Call Centers and the operation of the Zeitlin Entities.

BACKGROUND

3. PACs are entities registered with the Federal Election Commission ("FEC") that may be tax-exempt, and collect money to advocate on behalf of or against certain causes and political candidates. By contrast, charities, unlike PACs, typically provide direct services to communities or causes. Under federal law, independent expenditure-only PACs may raise unlimited contributions provided they do not make expenditures in coordination or in concert with any candidate for federal office or such a candidate's committee. PACs are required to file periodic reports with the FEC providing information about their fundraising and expenditures. Based on these reports, the FEC provides information about each PAC to the public through a searchable public database that shows, among other things, how much money is raised and spent by each PAC and how that money is spent.

4. RICHARD ZEITLIN, the defendant, has owned and operated telemarketing call centers (*i.e.*, the Zeitlin Call Centers) for decades, beginning in at least in or about 1994 when he created a particular entity ("Zeitlin Entity-1"). After Zeitlin Entity-1, ZEITLIN opened and operated a number of different entities (*i.e.*, the Zeitlin Entities), in connection with the Zeitlin Call Centers. In or about 2020, ZEITLIN effectively replaced certain of the Zeitlin Entities with new entities (together, the "New Zeitlin Entities"), also in connection with the Zeitlin Call Centers.

5. Initially, the Zeitlin Call Centers provided telemarketing services principally to charities. In or about 2017, however, RICHARD ZEITLIN, the defendant, decided to shift the business focus of the Zeitlin Call Centers from charity clients to PAC clients. As part of that shift, ZEITLIN encouraged certain prospective clients to operate PACs rather than charities. ZEITLIN transitioned to servicing primarily PACs in part to avoid certain regulations for charities and requirements associated with telemarketing for charities that do not apply to PACs.

6. The Zeitlin Call Centers employed call center employees or telemarketers in the United States and abroad to call potential donors and solicit financial contributions. These phone calls used either a live call center employee following a written script or pre-recorded portions of a script that a call center employee would play in response to statements made by the potential donor (such as playing, "Can I talk to your mom or dad please?" if a child answered the phone) so that the donor would believe they were having a conversation with a live telemarketer. In either case, PAC treasurers, who were responsible for their respective PACs, were led to believe they had ultimate approval over the call scripts used to solicit contributions. The Zeitlin Entities kept a substantial percentage of the funds raised by the Zeitlin Call Centers—typically approximately 90 percent. The remaining funds went to the charity or PAC on whose behalf the donations were made. As a result of this pay structure, the more funds the Zeitlin Call Centers raised for PACs and charities, the more money the Zeitlin Entities, and thus RICHARD ZEITLIN, the defendant, ultimately made.

ZEITLIN'S SCHEME TO DEFRAUD DONORS

7. From at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, defrauded donors and potential donors by directing employees of the Zeitlin Call Centers to make fundraising calls containing false and/or misleading statements that

misled donors and potential donors into believing that they were donating money (a) to a charity or direct-services organization rather than to a PAC; (b) that would go to an organization (rather than to the telemarketers); and/or (c) to support a "new" or "special" drive that was underway.

8. Specifically, from at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, directed employees of the Zeitlin Entities to alter the call scripts used when calling potential donors on behalf of certain PACs in order to mislead potential donors into believing that they would be giving to a direct-services organization (*i.e.*, a charity), rather than to a political advocacy organization, (*i.e.*, a PAC). ZEITLIN directed that these lies, misleading statements, and misrepresentations be made so that the donors would be more likely to give money as a result of the call, thereby increasing the funds raised and profits for the Zeitlin Entities. For instance, ZEITLIN directed employees to change call scripts to suggest that the organization soliciting donations performed direct services by, for example, telling a potential donor that "your support helps the handicapped and disabled veterans by working on getting them the medical needs the VA doesn't provide" and/or to remove references to "PAC" or "political action committee." Because of these misleading statements that ZEITLIN directed, donors were not aware that they were being solicited by and contributing money towards a PAC that focused on political advocacy rather than a charity that provided direct services.

9. For example, in or about 2018, RICHARD ZEITLIN, the defendant, and the Zeitlin Call Centers were hired by the treasurer of a certain PAC ("PAC Treasurer-1") to make solicitation calls on behalf of one of the above-referenced PACs ("PAC-1"). Recipients of fundraising calls from the Zeitlin Call Centers (*i.e.*, potential donors) reported that calls were being made on behalf of PAC-1 that portrayed the organization as a charity that provided certain direct services, including assisting veterans with medical services and housing, rather than as a PAC that engaged

in political activity. In response to reports from PAC Treasurer-1 about donor complaints, ZEITLIN falsely denied that such calls were being made on behalf of PAC-1. At or around the same time, however, ZEITLIN also acknowledged that calls describing PAC-1 as a charity or direct-services organization would be improper. In response to requests by PAC Treasurer-1 to produce recordings of solicitation calls, ZEITLIN refused to provide any such recordings.

10. Nonetheless, the Zeitlin Call Centers continued to make such misrepresentations at certain times when raising funds for certain PACs from at least in or about 2017 through at least in or about 2020. Based at least in part on the false and misleading representations directed and authorized by ZEITLIN, the Zeitlin Call Centers raised tens of millions of dollars in contributions.

11. Between at least in or about 2017 up to and including in or about 2018, RICHARD ZEITLIN, the defendant, also raised money through the Zeitlin Call Centers for certain PACs knowing that none of the money raised on behalf of those PACs would actually fund the PAC. ZEITLIN agreed with treasurers of certain PACs that one of ZEITLIN's entities ("Zeitlin Entity-2") would pay an advance of approximately $30,000 to certain of their PACs, and in exchange, 100 percent of the money subsequently raised by the Zeitlin Call Centers for those PACs over a specified time period (the "100% Time Periods") would be kept by Zeitlin Entity-2 (the "100% Agreements"). Despite the 100% Agreements, ZEITLIN and the Zeitlin Call Centers continued to make calls during the 100% Time Periods to potential donors on behalf of certain PACs falsely representing that donations would be used by those PACS, when in fact all of the money raised during the 100% Time Periods went to Zeitlin Entity-2 rather than to the organization or drive referenced on the fundraising call.

12. Between at least in or about 2017 up to and including in or about 2020, in order to increase funds raised and profits for the Zeitlin Entities, the Zeitlin Call Centers, with the approval

of RICHARD ZEITLIN, the defendant, falsely represented to potential donors that a "new" or "special" drive was "under way" and that their donation would help support the alleged new or special drive.

13. At various times relevant to this Indictment, RICHARD ZEITLIN, the defendant made multiple attempts to conceal his scheme and avoid attracting scrutiny from the public and investigating agencies relating to the Zeitlin Call Centers, the Zeitlin Entities, and ZEITLIN's scheme to defraud. For example:

a. Between at least in or about 2017 up to and including at least in or about 2020, ZEITLIN created various entities that appeared to provide different types of services to PACs from the Zeitlin Call Centers (*i.e.*, the Zeitlin Entities). In or about 2020, ZEITLIN created new entities to effectively replace certain of the existing Zeitlin Entities (*i.e.*, the New Zeitlin Entities). ZEITLIN selected certain of his employees to act as nominal owners of the New Zeitlin Entities even though ZEITLIN managed and controlled them.

b. As a result of ZEITLIN's efforts, invoices for services provided by the Zeitlin Call Centers listed payments owed by PACs to various of the Zeitlin Entities, rather than one entity. Likewise, publicly available FEC reports for PACs that used the Zeitlin Call Centers listed PAC payments made to multiple Zeitlin Entities rather than to one entity, and the PACs therefore appeared to pay different business rather than one business. In addition, ZEITLIN directed an employee to create fraudulent invoices billing certain PACs at an hourly or per-unit rate when, in truth and in fact, each entity was paid not by the hour, but rather, as part of ZEITLIN's overall collection of a large percentage of the money raised (typically approximately 90 percent).

c. On or about December 8, 2020, while testifying under oath during a deposition in connection with a federal civil matter, ZEITLIN falsely stated, in substance and in

part, that neither he nor employees of the Zeitlin Entities provided input as to the call scripts used by the Zeitlin Call Centers when making telemarketing calls on behalf of PACs. In truth and in fact, ZEITLIN and the employees of the Zeitlin Call Centers frequently provided input on and changed call scripts, including by adding false and misleading statements into the call scripts.

d. On or about March 31, 2022, in a declaration filed under penalty of perjury to a federal judge, ZEITLIN falsely stated that, among other things, he was not associated with and did not direct, supervise, or control certain of the New Zeitlin Entities. In truth and in fact, ZEITLIN controlled all the New Zeitlin Entities throughout their existence by exercising ultimate authority over managerial, operational, and financial decisions, including at the time he signed this declaration.

ZEITLIN'S ORDER TO DESTROY RECORDS

14. Beginning in or about 2018 to the present, RICHARD ZEITLIN, the defendant, has maintained a practice of principally communicating with employees of the Zeitlin Call Centers by phone or by encrypted messaging applications that typically delete data after a specified time period, or communicating with employees indirectly through an intermediary. For example, in or about 2018, ZEITLIN, directed certain employees of the Zeitlin Entities to delete materials and documents bearing ZEITLIN's name. In addition, ZEITLIN regularly received information about the operations of the business from CC-1 and relayed messages to others through CC-1.

15. On or about May 24, 2022, in connection with a federal investigation, law enforcement officers served federal grand jury subpoenas to certain individuals associated with the Zeitlin Entities and the PACs for which they solicited donations. On or about the same date, RICHARD ZEITLIN, the defendant, learned about the federal subpoenas and instructed CC-1 to delete his communications on a particularly electronic messaging application ("Application-1")

that Zeitlin's employees used internally to communicate with one another. ZEITLIN also instructed CC-1 to direct other of Zeitlin's employees to do the same. CC-1 relayed ZEITLIN's instruction to certain of Zeitlin's employees. The electronic messages that ZEITLIN instructed his employees to destroy contained internal communications among Zeitlin's employees about the Zeitlin Call Centers and the operations of the Zeitlin Entities, among other things.

STATUTORY ALLEGATIONS

COUNT ONE
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

16. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

17. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343, and did engage in the foregoing in connection with the conduct of telemarketing.

18. It was a part and an object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, ZEITLIN agreed with one or more others to engage in a scheme

to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1349 and 2326.)

COUNT TWO
(Wire Fraud)

The Grand Jury further charges:

19. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

20. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, ZEITLIN engaged in a scheme to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1343, 2326, and 2.)

COUNT THREE
(Conspiracy to Obstruct Justice)

The Grand Jury further charges:

21. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

22. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to obstruct justice, in violation of Title 18, United States Code, Section 1512(c).

23. It was a part and object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, would and did corruptly alter, destroy, mutilate, and conceal a record, document, and other object, and attempt to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise would and did corruptly obstruct, influence, and impede an official proceeding, and attempt to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Section 1512(c) and (k).)

COUNT FOUR
(Obstruction of Justice)

The Grand Jury further charges:

24. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

25. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, corruptly altered, destroyed, mutilated, and concealed a record, document, and other object, and attempted to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise corruptly obstructed, influenced, and impeded an official proceeding, and attempted to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Sections 1512(c) and 2.)

FORFEITURE ALLEGATION

26. As a result of committing the offenses alleged in Counts One and Two of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(8) and 2328, any and all real or personal property used or intended to be used to commit, to facilitate, or to promote the commission of said offenses; and any and all real or personal property constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of said offenses including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses, and any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offenses.

27. As a result of committing the offenses alleged in Counts Three and Four of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28 United States Code, Section 2461(c),

any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

28. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982 and 2328;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

FOREPERSON

DAMIAN WILLIAMS
United States Attorney

Exhibit B

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of Nevada

FILED
AUG 16 2023
U.S. MAGISTRATE JUDGE
BY:

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

7815 WEST LA MADRE WAY,
LAS VEGAS, NEVADA 89149

Case No. 2:23-MJ- 744-CF

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

7815 WEST LA MADRE WAY, LAS VEGAS, NEVADA 89149 (See Attachment A-1)

located in the _____ District of Nevada, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment B-1

I hereby attest and certify on 8/16/23 that the foregoing document is a full true and correct copy of the original on file in my office, and in my legal custody.

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA
By: _____ Deputy Secretary

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343,1349, 2326, 1512(c) & (k), and 2	Conspiracy to commit wire fraud; wire fraud; conspiracy to obstruct justice; obstruction of justice

The application is based on these facts:

See attached Affidavit and Exhibit 1

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kelsey Palermo
Applicant's signature

FBI Special Agent Kelsey Palermo
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 ~~by telephone~~ in person LC *(specify reliable electronic means).*

Date: 08/16/2023

CAM FERENBACH
Judge's signature

City and state: Las Vegas, Nevada

Honorable Cam Ferenbach
Printed name and title

JASON M. FRIERSON
United States Attorney
District of Nevada
Nevada Bar Number 7709
DAVID KIEBLER
Assistant United States Attorney
501 Las Vegas Boulevard South, Suite 1100
Las Vegas, Nevada 89101
Tel: (702) 388-6519
Fax: (702) 388-6418
David.Kiebler@usdoj.gov
Attorneys for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN THE MATTER OF THE SEARCH OF: 7815 WEST LA MADRE WAY, LAS VEGAS, NEVADA 89149	Case No. 2:23-MJ- 744 -VCF **Affidavit in Support of an Application for a Search Warrant** **(Under Seal)**
IN THE MATTER OF THE SEARCH OF: 1835 EAST CHARLESTON BOULEVARD, LAS VEGAS, NEVADA 89104	Case No. 2:23-MJ- 743 -VCF **Affidavit in Support of an Application for a Search Warrant** **(Under Seal)**

I, KELSEY PALERMO, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an application under Federal Rule of Criminal Procedure 41 for warrants to: (a) search a residential property that is located in the District of Nevada and further described in Attachment A-1, which is incorporated by reference herein: 7815 West La Madre Way, Las Vegas, Nevada 89149, located in Clark County, Nevada (hereafter, "**Subject Premises-1**"); (b) seize from **Subject Premises-1** evidence, fruits, and instrumentalities of the subject offenses described below and in Attachment B-1, which is

incorporated by reference herein, including certain electronic devices as described in Attachment B-1; (c) search a business property that is located in the District of Nevada and further described in Attachment A-2, which is incorporated by reference herein: 1835 East Charleston Boulevard, Las Vegas, Nevada 89104, located in Clark County, Nevada (hereafter, "**Subject Premises-2**," and together with Subject Premises-1, the "**Subject Premises**"); and (d) seize evidence, fruits, and instrumentalities of the subject offenses described below and in Attachment B-2, which is incorporated by reference herein, including certain electronic devices also described in Attachment B-2.

2. The Federal Bureau of Investigation ("FBI" or "Investigating Agency") is investigating fraud committed by Richard ZEITLIN and others through ZEITLIN's telemarketing call center business, which provided, and continues to provide, services to certain charities and political action committees ("PACs"). On or about August 15, 2023, a grand jury sitting in the Southern District of New York returned an Indictment (the "Indictment") charging ZEITLIN in three counts with: (1) conspiracy to commit wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1349 and 2326; (2) wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1343, 2326, and 2; (3) conspiracy to obstruct justice in or about May 2022, in violation of 18 U.S.C. § 1512(c), (k); and (4) obstruction of justice in or about May 2022, in violation of 18 U.S.C. § 1512(c) (together, the "Subject Offenses"). A copy of the Indictment is attached hereto as Exhibit 1 and is incorporated by reference herein. **Subject Premises-1** is ZEITLIN's residence, and **Subject Premises-2** is one of ZEITLIN's business locations. Based upon the investigation and as set forth in detail below, probable cause exists to believe that the **Subject Premises** contain evidence, fruits, and instrumentalities of the Subject Offenses.

AGENT BACKGROUND

3. I am a Special Agent with the FBI. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI for approximately eight years, and for three years before that I worked as a Staff Operations Specialist with the FBI. For more than one year, I have been assigned to a public corruption squad in the FBI's New York field office. Prior to the FBI's public corruption squad, I was assigned to an FBI counter-intelligence squad. As an FBI Special Agent, I have participated in numerous investigations involving public corruption offenses and fraud, including telemarketing fraud and wire fraud offenses. I have also participated in the execution of search warrants involving premises and electronic evidence. Through my training, education, and experience, I am familiar with the techniques and methods of operation commonly used by individuals engaged in fraud to communicate, operate their scheme(s), conceal their criminal activities, and avoid detection by law enforcement. I am also familiar with the means and methods commonly used by individuals who obstruct justice, including by destroying or deleting evidence and/or directing others to destroy or delete evidence.

4. As an FBI Special Agent, I have received training in the enforcement of federal laws pertaining to public corruption and fraud offenses, including: (1) debriefing defendants, witnesses, and informants, as well as others who have knowledge of public corruption offenses, obstruction offenses, and schemes to defraud, including wire fraud, telemarketing fraud, and frauds that involve PACs; (2) the planning, participation, and/or management of field operations such as surveillance, arrests, the interception of wire communications, and the execution of search warrants; (3) the acquisition, preservation, processing, and analysis of evidence; (4) the

seizure, search, and analysis of electronic devices and electronically stored information; and (5) the tracking of crime proceeds.

5. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. Unless explicitly stated otherwise, all descriptions of conversations are non-verbatim. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

TECHNICAL TERMS

6. Based on my training and experience, and information acquired from other law enforcement officials with technical experience, I know the terms described below have the following meanings:

a. "Electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, external hard drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

b. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually

contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Wireless telephones typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions. Tablets also contain apps.

d. A "storage medium" is any physical object upon which electronic data can be recorded. Examples include USB flash drives, hard disks, RAM, flash memory, CD-ROMs, and other magnetic or optical media.

e. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user

driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

i. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

j. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

k. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of

an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

l. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

m. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

n. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

PROBABLE CAUSE

THE SUBJECT OFFENSES

7. As set forth above, on or about August 15, 2023, a grand jury sitting in the Southern District of New York returned the Indictment, charging ZEITLIN with the Subject Offenses. The Indictment is incorporated by reference herein.

8. As set forth in the Indictment:

a. PACs are entities registered with the Federal Election Commission ("FEC") that may be tax-exempt, and collect money to advocate on behalf of or against certain causes and political candidates. By contrast, charities, unlike PACs, typically provide direct services to communities or causes. Under federal law, independent expenditure-only PACs may raise unlimited contributions provided they do not make expenditures in coordination or in concert with any candidate for federal office or such a candidate's committee. PACs are required to file periodic reports with the FEC providing information about their fundraising and expenditures. Based on these reports, the FEC provides information about each PAC to the public through a searchable public database that shows, among other things, how much money is raised and spent by each PAC and how that money is spent. (Indictment ¶ 3).

b. ZEITLIN has controlled and operated telemarketing call centers (the "Zeitlin Call Centers") for decades, including from at least in or about 1994 to in or about 2023. The Zeitlin Call Centers have raised at least approximately hundreds of millions of dollars for charities and PACs through at least approximately hundreds of thousands of calls to donors and potential donors and various entities that ZEITLIN controlled (the "Zeitlin Entities"). (*Id.* ¶ 1).

c. Initially, the Zeitlin Call Centers provided telemarketing services principally to charities. In or about 2017, however, ZEITLIN decided to shift the business focus of the Zeitlin Call Centers from charity clients to PAC clients. As part of that shift, ZEITLIN

encouraged certain prospective clients to operate PACs rather than charities. ZEITLIN transitioned to servicing primarily PACs in part to avoid certain regulations for charities and requirements associated with telemarketing for charities that do not apply to PACs. (*Id.* ¶ 5).

d. From at least in or about 2017 through at least in or about 2020, ZEITLIN used the Zeitlin Call Centers to defraud numerous donors and potential donors by providing misleading and false information about how the donors' money would be spent and the nature of the organizations to which they were giving. For example, ZEITLIN directed his employees to make calls on behalf of certain PACs that falsely portrayed the PAC as a charity and/or a direct-services organization rather than as a PAC. Even after receiving complaints that the Zeitlin Call Centers were providing false and misleading information to donors and potential donors during fundraising calls, ZEITLIN continued his fraudulent scheme and made efforts to conceal it. The Zeitlin Entities profited from ZEITLIN's fraud, typically keeping a large portion of each dollar donated—approximately 90 percent—the rest of which was disbursed to the respective PAC. (*Id.* ¶ 1).

e. For a period between in or about 2017 and 2018, ZEITLIN entered into agreements with the owner of two PACs to give those PACs a $30,000 advance in exchange for keeping 100% of the money he raised, notwithstanding the fact that ZEITLIN represented to donors during this period that their contributions would help the PAC. (*Id.* ¶ 11).

f. In or about May 2022, after learning that he and the Zeitlin Entities were under federal investigation, ZEITLIN directed at least one of his employees ("CC-1") to instruct other employees of the Zeitlin Entities to delete electronic messages relating to the Zeitlin Call Centers and the operation of the Zeitlin Entities. (*Id.* ¶ 2).

9. Based on my participation in this investigation, including my participation in interviews of former and current ZEITLIN employees, and my review of documents and records, I know the following, among other things:

a. In or about 1994, ZEITLIN created a particular entity for his call center business called Courtesy Call. ZEITLIN has since replaced Courtesy Call and created numerous additional entities (the "Zeitlin Entities") in connection with his call center business. In or about 2020, ZEITLIN replaced his existing entities and created new entities (the "New Zeitlin Entities") in connection with his call center business, enlisting employees and associates to act as the owners of the New Zeitlin Entities even though ZEITLIN continued to direct, supervise, and control them.

b. The Zeitlin Entities and New Zeitlin Entities include, among others: Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. ZEITLIN had pre-existing relationships with certain of his PAC clients. For example, he is close friends with an individual who is the owner/treasurer of at least approximately three PACs that used the Zeitlin Call Centers to raise funds (*i.e.*, ZEITLIN was the best man at his wedding and is the godfather of his child).

d. ZEITLIN is believed to have compensated certain of his employees in a manner that does not immediately appear to be commensurate with their education and experience, at least in part to secure their reliance on ZEITLIN with respect to their livelihood.

THE SUBJECT PREMISES

10. Based on my training and experience, I know that when an individual participates in a criminal scheme, including a scheme to defraud, that individual often maintains documentary evidence of the scheme in their home, including photographs evidencing their relationship with co-conspirators, witnesses, or associates; financial records showing transactions that are evidence of criminal conduct; and business records, including original records, relating to the creation, operation, ownership, development, control, and dissolution of entities used or related to the scheme. I also know that such documentary evidence is frequently stored on electronic devices such as laptop computers, desktop computers, or other electronic storage devices. I also submit there is probable cause that Subject Premises-1 will contain hard-copy and original financial and business records, such as documents establishing certain business entities and bank statements evidencing relevant transactions, as well as electronic files and copies of financial and business records and communications between ZEITLIN and co-conspirators and witnesses, which are likely stored on electronic devices found in or on Subject Premises-1.

11. Based on my training and experience, I know that senior executives, senior managers, and owners of businesses commonly work from home and/or have home offices because of the nature of their roles and responsibilities, which typically require the individual to work after-hours and on the weekends, the need to access certain business and financial documents after-hours in order to operate and manage their businesses, the need to protect certain important, confidential, or sensitive business and financial records, the individual's ability to more freely determine from where he or she will work (*i.e.*, when they will work remotely), the increased frequency and/or necessity of business travel for the individual because of his or her role (and thus the need to carry more work-related materials home), and the increased frequency of personal travel for the individual because he or she may have the resources and flexibility to

do so. I also know that following the COVID-19 pandemic's height in or about early 2020, many Americans began working more frequently from home or remotely. As a result, senior executives, managers, and owners of businesses commonly possess and retain business-related documents within their homes.

12. Based on my training and experience, I know the following, in substance and in part, concerning the use of electronic devices and electronic evidence in criminal schemes:

a. Individuals engaged in fraud typically utilize electronic equipment such as computers, software programs, cellular telephones, mobile applications, and other electronic devices to further facilitate their illicit scheme.

b. Individuals who participate in criminal schemes, such as schemes to defraud and schemes to destroy evidence, commonly use electronic communications to communicate with co-conspirators, establish and use online financial accounts, keep track of co-conspirator information; and keep a record of illegal transactions or criminal proceeds for future reference.

c. When an individual participates in a criminal scheme, photographs or videos stored in that individual's cellphone(s) and other electronic devices often contain evidence of that scheme because such photographs or videos can provide evidence of relationships between participants in the scheme and the time and/or location of meetings between co-conspirators.

d. When an individual participates in a criminal scheme, that individual's web browser history often contains evidence of that scheme. For example, individuals who engage in schemes to defraud who seek to avoid law enforcement detection may conduct research on relevant legal rules and regulations. Here, for instance, ZEITLIN may have conducted research on FEC regulations, telemarketing regulations, PAC regulations, charity regulations, and state and federal laws pertaining to telemarketing and fraud. Likewise, individuals who engage in

methods to avoid law enforcement detection—including, for example, by reducing electronic communications or communicating through encrypted applications—may have conducted research on encryption, applications and devices that encrypt communications, and applications that do not save or store data. Finally, individuals who seek to destroy evidence may research technical mechanisms to permanently delete electronic evidence so that it may not be recovered.

e. Historical location data collected by a user's cellphone(s) and other electronic devices can be relevant to establishing that user's participation in a criminal conspiracy, such as by showing when the relevant actors were together in person and thus how and when information was transmitted.

f. Individuals who engage in criminal schemes commonly maintain electronic records relating to their schemes, such as contact information for co-conspirators, records of illegal transactions or criminal proceeds, and financial account statements. These materials can be easily moved between an individual's electronic devices and storage accounts, such as by email and file sharing and transfers between devices and accounts.

g. Electronic communications platforms, like email, text messages, and Signal, can often be accessed from multiple devices like a user's mobile devices and desktop computer. Based on my interviews with several Zeitlin Call Center employees, I know that Zeitlin communicated with his employees through Signal and occasionally through email. Based on my review of publicly available information, I know that a single Signal account can be accessed from a mobile device and desktop computer.[1]

[1] *See Installing Signal*, Signal.com, https://support.signal.org/hc/en-us/articles/360008216551-Installing-Signal ("You can link Signal Desktop to your mobile device to send and receive Signal messages from your laptop or desktop computer.").

h. Where electronic messages or other electronic files are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because electronic files can be stored on cellphones or other electronic devices or computer servers for years at little or no cost and users thus may have little incentive to delete data that may be useful to consult in the future.

13. Based on my training and experience, I know that cellphones are frequently kept at the owner's residence and/or on their owner's person where the owner has immediately access to them. I also know that individuals who own cellphones often backup or sync the data on those cellphones to other electronic devices such as laptop computers, desktop computers, or other electronic storage devices.

14. Based on my training and experience and my participation in this investigation, I know that even individuals who have destroyed or have attempted to destroy evidence, and individuals who attempt to evade law enforcement detection by reducing the use of non-encrypted communications, may not know what evidence is relevant or important to law enforcement and how to permanently delete evidence.

Subject Premises-1

15. I believe that ZEITLIN resides at **Subject Premises-1** based on the following, among other things:

a. Based on my review of publicly available information, including records from an online business portal provided by the Nevada Secretary of State ("SilverFlume"), I know that Unified Data Services LLC, one of the Zeitlin Entities, was formed on or about August 15, 2018, and listed ZEITLIN as a "Manager" with **Subject Premises-1** as ZEITLIN's address.

b. On or about April 18, 2023, the Honorable Jennifer E. Willis, U.S. Magistrate Judge, Southern District of New York, issued a warrant (the "SCA Warrant") for all

content and other information associated with the Google Account with email address "ccirickz@gmail.com," an account believed to be used by ZEITLIN ("Zeitlin Email-1").[2] Based on my review of emails and records produced by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, my participation in this investigation, and my conversations with other law enforcement officers, I know the following, among other things:

i. On or about January 30, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Mon, Jan 30," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject Premises-1**, including an envelope from a P.O. Box in San Antonio, Texas; a tax document from one of the New Zeitlin Entities, "LAV Services LLC," in Cedar City, Utah; and a "Pre-Paid Service Notice" for "Heating System Check" and "Water Heater Inspection and Flush" addressed to "Rick & Luliana [sic] Zeitlan [sic]" (all caps in the original). I believe "Liliana Zeitlin" is the name of ZEITLIN's current or former spouse, from whom ZEITLIN is either separated or divorced.[3]

ii. On or about March 15, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Wed, Mar 15," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject**

---

[2] The SCA Warrant authorized the search of records associated with several email addresses, including Zeitlin Email-1 and a second email address used be Zeitlin, "rickz@advancedtci.com" ("Zeitlin Email-2").

[3] This email also included images of tax documents addressed to "Jordan Zeitlin" at **Subject Premises-1** (all caps in the original) and Sarah H Zeitlin" at **Subject Premises-1** (all caps in the original).

Premises-1, including an envelope marked "Reservations" and "Personal and Confidential" (all caps in the original).[4]

iii. On or about April 5, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Wed, Apr 5," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject Premises-1**, including an envelope from SiriusXM, an envelope from Charles Schwab, an envelope from Capital Bank, and two envelopes from Las Vegas Valley Water District (addressed to "Zeitlin, Liliana" and "Zeitlin, Richard L").

16. Based on my review of records provided by the U.S. Postal Service, my participation in this investigation, and my conversations with other law enforcement officers, I know, among other things, that on or about July 12, 2023, U.S. mail addressed to ZEITLIN on behalf of "Advance Telephony LLC," one of the Zeitlin Entities, was delivered to **Subject Premises-1**. I believed "Advance Telephony LLC" is a reference to Advanced Telephony Consultants, one of the Zeitlin Entities set forth above.[5]

17. On or about August 10, 2023, the Honorable Gabriel W. Gorenstein, U.S. District Judge, Southern District of New York, issued a warrant (the "GPS Warrant") for prospective and historical location information and pen register information for the cellphone assigned call

---

[4] The email also included images of two tax documents enclosed with a perforated seal from "LAV SERVICES LLC" addressed to "Sheryl Teller" at "615 Crescent Lane" in "Thiensville WI." Based on my review of law enforcement databases, I understand that "Sheryl Teller" has previously used the last name "Zeitlin," and accordingly may be a relative of ZEITLIN. The recipient name and address on these tax documents (*i.e.*, the name Sheryl Teller" and the address below) is typed in a different font and size than the recipient name and address on the tax documents referenced above, and appears to have been typed and printed and affixed to these documents on top of the original recipient name and address.

[5] Based on my participation in this investigation, I also know that ZEITLIN owns other properties, including a residence in Mexico.

number 702-241-3310, a phone number subscribed in the name of Richard Zeitlin and believed to be used by ZEITLIN ("Zeitlin Phone-1").

a. Based on data and information provided by Verizon Wireless, as of the evening of on or about August 13, 2023, Zeitlin Phone-1 was located in the vicinity of **Subject Premises-1**.

18. Based on my review of documents and records provided by Apple in or about August 2023, I know that as of in or about August 2023, several Apple electronic devices were associated with Zeitlin Phone-1. These devices were activated between in or about May 2010 through in or about March 2023, and include Apple iPhones, iPads, iPods, TVs, iMac desktop computers, and Macbook laptops.

19. As discussed above, I know that owners, senior executives, and senior managers of businesses often work remotely and/or work from home. Based on my participation in this investigation, including my participation in interviews of [redacted], I know that ZEITLIN regularly conducted business by phone—that is, from outside of a business office—in addition to, at times, meeting in person with certain Zeitlin employees, including at **Subject Premises-2** and an office in the Whitney Ranch neighborhood of Henderson, Nevada (the "Whitney Ranch Office"). ZEITLIN communicated with

[redacted][6]

employees, principally CC-1, by phone or encrypted messaging application. I also know that many of Zeitlin's employees also worked remotely and/or from home.

20. Based on my review of a page on Zillow.com, a website that shows current and historical real estate listings, I have reviewed a real estate posting for **Subject Premises-1**, which included several photographs of what I believe to be **Subject Premises-1**.[7] One of the photographs, shown below, appears to show a home office inside **Subject Premises-1**:

The photograph above has a mark in the bottom left part of the screen that says "LVR 2022," which, based on my training and experience, shows that the photograph was created in or about 2022.[8]

[7] *See* 7815 W La Madre Way, Las Vegas, NV 89149, Zillow, https://www.zillow.com/homedetails/7815-W-La-Madre-Way-Las-Vegas-NV-89149/6900730_zpid/ (last visited Aug. 11, 2023).

[8] Attachment A-1 includes two photographs of ZEITLIN that that were included in grand jury subpoena returns for a financial account controlled by ZEITLIN. The two photographs of ZEITLIN in Attachment A-1 appear to show ZEITLIN seated at the desk shown in the above photograph of **Subject Premises-1**, based on my review of the three photographs.

21. Based on my review of data and records provided by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, I have learned that ZEITLIN has had the following online activity, among other activity:

a. On or about April 3, 2023, ZEITLIN accessed the website for Wells Fargo, a national bank.

b. On or about April 2, 2023, ZEITLIN visited a webpage titled "Leaving the US While Indicted" using a Google Chrome web browser.

c. On or about March 16, 2023, ZEITLIN visited the website for Citibank, a national bank.

d. On or about March 14, 2023, ZEITLIN accessed an email in his Google email account with the subject line "FEC hotline number."

e. On or about March 9, 2023, ZEITLIN visited webpages on the FEC website titled "FEC | Nonconnected | Notices required on PAC solicitations" and "Nonconnected committee webstore/fundraiser disclaimer example."

f. On or about March 8, 2023, ZEITLIN visited a webpage on the FEC website titled "FEC | Nonconnected | Notices required on PAC solicitations" and search on Google for the phrase "notices required on non connected pac solicitations."

22. Based on the foregoing, I believe there is probable cause to believe that **Subject Premises-1** will contain evidence, fruits, and instrumentalities of the Subject Offenses, including electronic devices.

Subject Premises-2

23. I know **Subject Premises-2** continues to be used by employees of the Zeitlin Call Centers to conduct the work of the Zeitlin Call Centers for the following reasons, among others:

a. Based on my participation in this investigation and my review of a transcript of a deposition of ZEITLIN in connection with a federal civil lawsuit, I know that on or about December 8, 2020, ZEITLIN stated the following, in substance and in part, under oath:

i. ZEITLIN owns a real estate company called "MRZ Management" that manages approximately two properties: **Subject Premises-2** and a property at 1009 Whitney Ranch Drive in Henderson, Nevada (*i.e.*, the Whitney Ranch Office, referenced above).

ii. Courtesy Call, the entity associated with the Zeitlin Call Centers, and Donor Relations, another entity associated with the Zeitlin Call Centers, were headquartered at **Subject Premises-2** up until in or about 2018. As of in or about 2020, a company that ZEITLIN partially owns, Chrome Builders Construction, formally operated out of **Subject Premises-2**.

b. Based on my participation in this investigation, including my participation in interviews of [redacted] know that **Subject Premises-2** is commonly referred to as the "Charleston" office because it is located on Charleston Boulevard

c. Based on my review of electronic messages provided to the Government in response to a grand jury subpoena, I know that on or about June 15, 2022, an employee of the Zeitlin Call Centers ("Employee-1") communicated with an individual who provides IT services to the Zeitlin Call Centers (*i.e.*, Employee-2) about **Subject Premises-2** via a communications application called Skype. Specifically, Employee-1 wrote to Employee-2 that two other employees ("Employee-3" and "Employee-4") needed office space at **Subject Premises-2**. Employee-1 and Employee-2 had the following exchange:

> Employee-1: [Employee-3] and [Employee-4] need an office at Charleston [*i.e.*, **Subject Premises-2**] to work in so he can teach her how to help him with scripting. It will take at least a month, maybe 2. Is anything available there?

Employee-2: yes/no lol

Employee-2: do they need a quiet place?

Employee-2: or will they be ok in a big open room

Employee-2: we were going to stick the couple people in the big open IT area []

. . .

Employee-1: It should work, they won't be recording, just putting everything together.

Employee-2: ok that was the plan was to put 4 desks in chrome… One for ["Employee-5"] and one for ["Employee-6"] and 2 for whatever else

Employee-2: looks like movers will be at the office on the 24th…

Employee-2: so need to make sure everyone has packed all their personal shit and gotten it out of there

Employee-1: What's a good date to tell [Employee-3's first name] and [Employee-4's first name] they can start at Charleston?

Employee-2: lets get through this move first cuz [sic] I have to find/source build 2 computers for them it will be fun

Employee-1: They were just going to move their computers from home to the office and then back when done. Just need a place to set it up.

Employee-2: ohh in that case the week after we move should be perfectly fine

Employee-2: ill [sic] make sure there is a power strip and a hot network cable for them

Based on my participation in this investigation and my conversations with other law enforcement officers, when Employee-2 wrote that "the plan was to put 4 desks in chrome," I understand Employee-2 was communicating, in substance and in part, that **Subject Premises-2** is the formal

office space for ZEITLIN's business, Chrome Builders Construction (*i.e.*, "chrome"), but Employee-2 was planning to put four desks in **Subject Premises-2** that employees of the Zeitlin Call Centers could use.[9]

[redacted]

[9] I am not aware of any evidence suggesting that Employee-1, Employee-2, or Employee-3 have done any work for Chrome Builders Construction.

[redacted]

18 _____

19 [10] [redacted]

20 [11] [redacted]

21

22

23

24

24. Based on my review of records provided by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, I have learned that Zeitlin had the following online activity, among other activity: On or about February 21, 2023, Zeitlin searched for, among others, the phrases: "1835 e charleston blvd las vegas assesors," "1835 e charleston blvd las vegas," and "clark county assessor 1835 E." Each of these searches references the address for **Subject Premises-2**.

25. Based on my experience and training and my participation in this investigation, I know that the vast majority of businesses use electronic devices, including computers. Here, I know that employees of the Zeitlin Call Centers regularly used electronic devices in their work and that call centers scripts and recordings were created, edited, shared, and circulated electronically. I also know that when employees of a business and/or entity, such as the Zeitlin Call Centers, continue to use an office space, desk, or workspace, formally or informally, work relating to that business or entity, including the work of those employees, typically remains at that office space.

26. Based on the foregoing, I believe there is probable cause to believe that **Subject Premises-2** will contain evidence, fruits, and instrumentalities of the Subject Offenses, including electronic devices.

SEIZURE OF ELECTRONIC DEVICES

27. As described above and in Attachments A-1, A-2, B-1, and B-2, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information

[redacted]

that might be found at the **Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on electronic devices. Thus, the applied-for warrant would authorize the search of the **Subject Premises**, as described in Attachment A-1 and A-2 to this Affidavit and to the Search Warrant, for the items described in Attachment B-1 and B-2 to this Affidavit and to the Search Warrant, including the seizure of electronic devices believed to be used by ZEITLIN and/or by employees and/or associates of the Zeitlin Entities and/or the Zeitlin Call Centers, including computers, cellphones, and electronic storage media, and potentially, the copying of such electronic devices and electronically stored information ("ESI"), under Rule 41(e)(2)(B).

28. Based on my training and experience and my participation in this investigation, including my review of the evidence gathered in this investigation, my review of data, reports, and records, my participation in interviews of witnesses, and my conversations with other law enforcement officers, and for the reasons set forth in this Affidavit, I submit that if an electronic device is found at the **Subject Premises**, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the Subject Offenses will be found on those electronic devices.

29. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic

storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

30. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any electronic devices, including computer devices, storage media, and cellphones, or potentially copy such electronic devices, and then transport the seized electronic devices to the Southern District of New York as described further below. The seizure of the electronic device is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

31. **Subject Premises-1** is a residence at which individuals other than ZEITLIN may reside. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on scene which electronic devices have been and/or are used by

ZEITLIN and which electronic devices have not been used by ZEITLIN, for example, based on the location of the device.

32. **Subject Premises-2** is a business location at which employees of ZEITLIN and the Zeitlin Call Centers have worked and are believed to continue to work. As discussed herein, the Zeitlin Call Centers (the "Company"), which is associated with numerous business entities, appears to be a functioning company that conducts some legitimate business. The seizure of the Company's computers or other storage media may limit the Company's ability to conduct its legitimate business. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on the scene what computers or storage media have been used by ZEITLIN and/or associates and/or employees of ZEITLIN in connection with the Zeitlin Call Centers and/or the Zeitlin Entities, as well as what electronic devices must be seized or may be copied, based on the location of the electronic devices, materials surrounding the electronic devices, and any markings on the electronic devices. Law enforcement personnel may speak with Company personnel on the scene as may be appropriate to determine the user(s) of the electronic devices. Where appropriate, law enforcement personnel will copy data, rather than physically seize computers, to reduce the extent of any disruption of the Company's business operations. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continued functioning of the Company's legitimate business. If, after inspecting the seized computers off-site, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the Government will return it.

33. Following seizure of any electronic devices, including cellphones, computer devices, and storage media from the **Subject Premises** and/or the creation of forensic image copies, the FBI intends to transport the electronic devices to the Southern District of New York

and seek judicial authority to search any electronically stored information contained therein for evidence of the Subject Offenses.

CONCLUSION

34. I respectfully submit that this affidavit supports probable cause to search the **Subject Premises** as described in Attachment A- and Attachment A-2 to this Affidavit and to the warrants and seize the items listed in Attachment B-1 and Attachment B-2 to this Affidavit and to the warrants, including electronic devices.

35. In light of the confidential nature of this investigation, and the fact that premature disclosure of this Affidavit could alert subjects of the investigation as to the nature and scope of the investigation, thereby prompting them to destroy evidence, shape their testimony, or tamper with witnesses, I respectfully request that the Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise and with the exception of the Government's disclosures pursuant to its discovery and disclosure obligations.

KELSEY PALERMO
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 X by telephone in person on the 16th day of August, 2023.

CAM FERENBACH
HONORABLE CAM FERENBACH
UNITED STATES MAGISTRATE JUDGE

I hereby attest and certify on 8/16/23 that the foregoing document is a full true and correct copy of the original on file in my office, and in my legal custody.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEVADA
CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA
By _____ Deputy Secretary

ATTACHMENT A-1

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 7815 West La Madre Way, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-1"), particularly described as a residential property that is surrounded by a solid white wall, with the numbers "7815" facing La Madre Way, and a black or dark grey gate. Inside the wall is a residence that is approximately 9,257 square feet. The residence's exterior is white, with accents and structures that are black, tan, and grey.

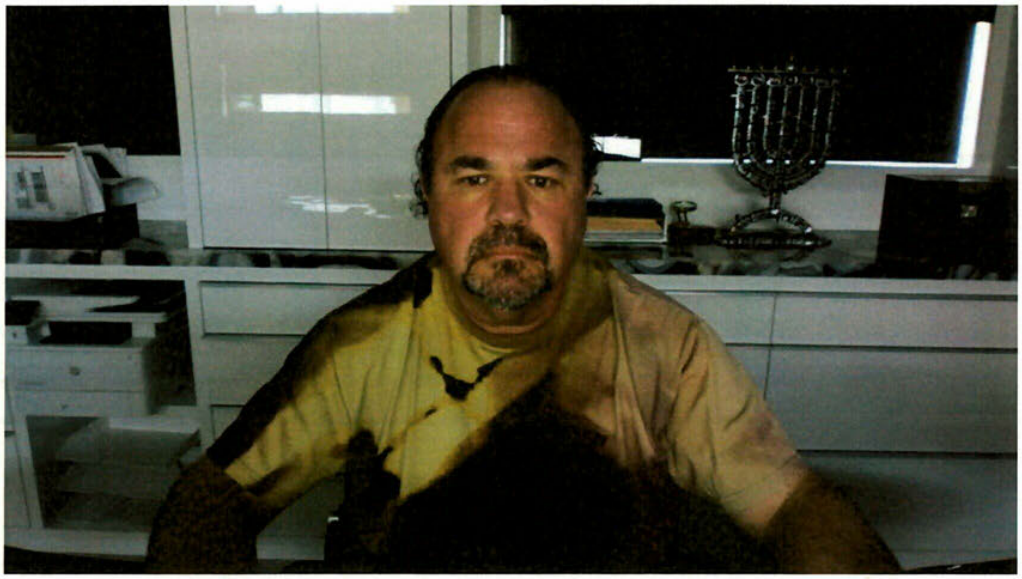
An image of the outside of Subject Premises-1 is below:

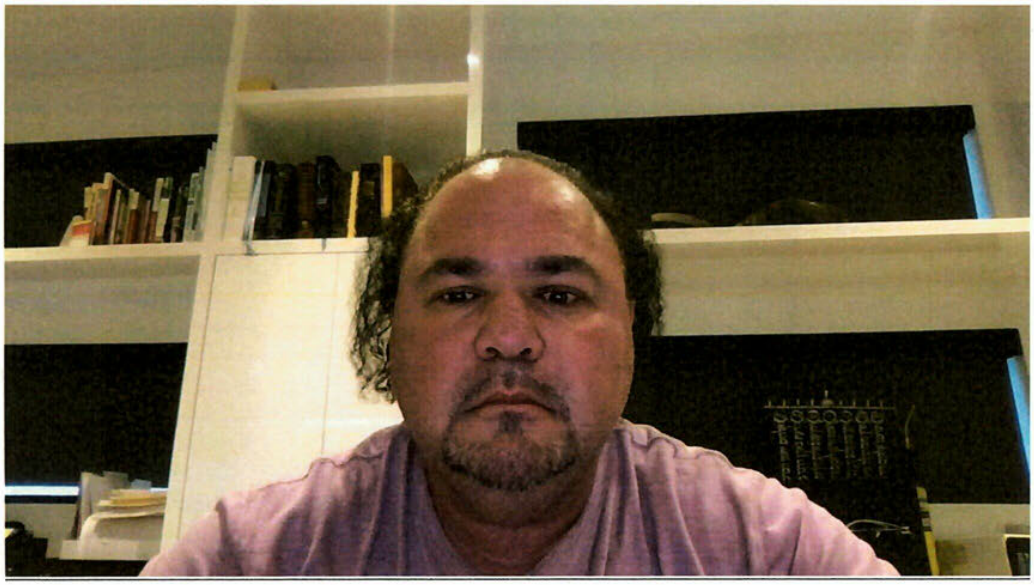
An image of an aerial view of Subject Premises-1 is below, with Subject Premises-1 highlighted with a red box:

The search of Subject Premises-1 shall include any and all attachments, storage units, casitas, pool houses, and appurtenances thereto, and all other areas within the curtilage. The search of Subject Premises-1 shall also include a search of any and all containers, locked containers, clothing, and personal items (*e.g.*, safes, electronic devices, backpacks, wallets, briefcases, and bags) within Subject Premises-1 at the time of the execution of the search warrant.

The search of Subject Premises-1 shall also include a search of the person of Richard Zeitlin, who was born on November 11, 1970, provided he is located at Subject Premises-1, specifically for the items listed in Attachment B. The search shall not include a body cavity or strip search of any person in the Subject Premises.

Two photographs of Richard Zeitlin are below:





ATTACHMENT A-2

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 1835 East Charleston Boulevard, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-2"), particularly described as a commercial property with a reddish-brown brick exterior, windows with white window frames, and a flat white awning that reads "CHARLESTON PROFESSIONAL BUILDING" in dark blue print on the left and "GENERAL CONTRACTOR" in lighter blue print on the right when facing Subject Premises-2. A white rectangular placard with the numbers "1835" in white sits above the white awning and is affixed to a white architectural structure with columns and grating. In front of Subject Premises-2 are approximately six parking spaces for vehicles to park perpendicular to the street in front of Subject Premises-2. The door to Subject Premises-2 is white and below and offset to the left of the portion of the awning that reads "GENERAL CONTRACTOR."

Two images of Subject Premises-2 are below with the white door highlighted with a red circle in the second image below. Subject Premises-2 does not include the orange building depicted in the images below that is to the right of Subject Premises-2 and marked with a placard reflecting a street number of "1837."


1900 E Charleston Blvd
Las Vegas, Nevada
WE FIX PHONES
FOR LEASE
BUILD TO SUIT
3B7 PHONE HOUSE
CHARLESTON PROFESSIONAL BUILDING
GENERAL CONTRACTOR
LIQUIDATION
Google


Las Vegas, Nevada
FOR LEASE
IMMEDIATE OCCUPANCY
UTILITIES INCLUDED
NO CAMS
BUILD TO SUIT
702 278 1275
CHARLESTON
BUILDING
GENERAL CONTRACTOR
1837
Google

ATTACHMENT B-1

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-1

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-1 by Richard Zeitlin, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to Zeitlin's call center business and its operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among Subjects, co-conspirators, witnesses, current and former clients, and current and former employees and/or associates, including but not limited to communications, photographs and evidence regarding their social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACs, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appear to have been used by Zeitlin and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin, including Apple electronic devices.

v. Any and all electronic devices associated with or that appear to be associated with the phone number 702-247-3310.

w. Any and all electronic devices associated with or that appear to be associated with either or both of the following email addresses: "ccirickz@gmail.com" and/or "rickz@advancedtci.com".

x. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

ATTACHMENT B-2

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-2

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-2, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Richard Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to call centers associated with and/or operated by Zeitlin and their operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among co-conspirators and witnesses, including but not communications, limited to social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACS, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appears to have been used by Zeitlin and current and former employees and/or associates of Zeitlin, and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin.

v. A black and silver computer monitor and computer tower that is believed to have been used by and/or appears to have been used by a former employee of Zeitlin.

w. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

RICHARD ZEITLIN,

Defendant.

SEALED INDICTMENT

23 Cr. _____ (___)

23 CRIM 419

The Grand Jury charges:

OVERVIEW

1. RICHARD ZEITLIN, the defendant, has controlled and operated telemarketing call centers (the "Zeitlin Call Centers") for decades, including from at least in or about 1994 to in or about 2023. The Zeitlin Call Centers have raised at least approximately hundreds of millions of dollars for charities and political action committees ("PACs") through at least approximately hundreds of thousands of calls to donors and potential donors and various entities that ZEITLIN controlled (the "Zeitlin Entities"). From at least in or about 2017 through at least in or about 2020, ZEITLIN used the Zeitlin Call Centers to defraud numerous donors and potential donors by providing misleading and false information about how the donors' money would be spent and the nature of the organizations to which they were giving. For example, ZEITLIN directed his employees to make calls on behalf of certain PACs that falsely portrayed the PAC as a charity and/or a direct-services organization rather than as a PAC. Even after receiving complaints that the Zeitlin Call Centers were providing false and misleading information to donors and potential donors during fundraising calls, ZEITLIN continued his fraudulent scheme and made efforts to conceal it. The Zeitlin Entities profited from ZEITLIN's fraud, typically keeping a large portion

of each dollar donated—approximately 90 percent—the rest of which was disbursed to the respective PAC.

2. In or about May 2022, after learning that he and the Zeitlin Entities were under federal investigation, RICHARD ZEITLIN, the defendant, directed at least one of his employees ("CC-1") to instruct other employees of the Zeitlin Entities to delete electronic messages relating to the Zeitlin Call Centers and the operation of the Zeitlin Entities.

BACKGROUND

3. PACs are entities registered with the Federal Election Commission ("FEC") that may be tax-exempt, and collect money to advocate on behalf of or against certain causes and political candidates. By contrast, charities, unlike PACs, typically provide direct services to communities or causes. Under federal law, independent expenditure-only PACs may raise unlimited contributions provided they do not make expenditures in coordination or in concert with any candidate for federal office or such a candidate's committee. PACs are required to file periodic reports with the FEC providing information about their fundraising and expenditures. Based on these reports, the FEC provides information about each PAC to the public through a searchable public database that shows, among other things, how much money is raised and spent by each PAC and how that money is spent.

4. RICHARD ZEITLIN, the defendant, has owned and operated telemarketing call centers (*i.e.*, the Zeitlin Call Centers) for decades, beginning in at least in or about 1994 when he created a particular entity ("Zeitlin Entity-1"). After Zeitlin Entity-1, ZEITLIN opened and operated a number of different entities (*i.e.*, the Zeitlin Entities), in connection with the Zeitlin Call Centers. In or about 2020, ZEITLIN effectively replaced certain of the Zeitlin Entities with new entities (together, the "New Zeitlin Entities"), also in connection with the Zeitlin Call Centers.

5. Initially, the Zeitlin Call Centers provided telemarketing services principally to charities. In or about 2017, however, RICHARD ZEITLIN, the defendant, decided to shift the business focus of the Zeitlin Call Centers from charity clients to PAC clients. As part of that shift, ZEITLIN encouraged certain prospective clients to operate PACs rather than charities. ZEITLIN transitioned to servicing primarily PACs in part to avoid certain regulations for charities and requirements associated with telemarketing for charities that do not apply to PACs.

6. The Zeitlin Call Centers employed call center employees or telemarketers in the United States and abroad to call potential donors and solicit financial contributions. These phone calls used either a live call center employee following a written script or pre-recorded portions of a script that a call center employee would play in response to statements made by the potential donor (such as playing, "Can I talk to your mom or dad please?" if a child answered the phone) so that the donor would believe they were having a conversation with a live telemarketer. In either case, PAC treasurers, who were responsible for their respective PACs, were led to believe they had ultimate approval over the call scripts used to solicit contributions. The Zeitlin Entities kept a substantial percentage of the funds raised by the Zeitlin Call Centers—typically approximately 90 percent. The remaining funds went to the charity or PAC on whose behalf the donations were made. As a result of this pay structure, the more funds the Zeitlin Call Centers raised for PACs and charities, the more money the Zeitlin Entities, and thus RICHARD ZEITLIN, the defendant, ultimately made.

ZEITLIN'S SCHEME TO DEFRAUD DONORS

7. From at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, defrauded donors and potential donors by directing employees of the Zeitlin Call Centers to make fundraising calls containing false and/or misleading statements that

misled donors and potential donors into believing that they were donating money (a) to a charity or direct-services organization rather than to a PAC; (b) that would go to an organization (rather than to the telemarketers); and/or (c) to support a "new" or "special" drive that was underway.

8. Specifically, from at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, directed employees of the Zeitlin Entities to alter the call scripts used when calling potential donors on behalf of certain PACs in order to mislead potential donors into believing that they would be giving to a direct-services organization (*i.e.*, a charity), rather than to a political advocacy organization, (*i.e.*, a PAC). ZEITLIN directed that these lies, misleading statements, and misrepresentations be made so that the donors would be more likely to give money as a result of the call, thereby increasing the funds raised and profits for the Zeitlin Entities. For instance, ZEITLIN directed employees to change call scripts to suggest that the organization soliciting donations performed direct services by, for example, telling a potential donor that "your support helps the handicapped and disabled veterans by working on getting them the medical needs the VA doesn't provide" and/or to remove references to "PAC" or "political action committee." Because of these misleading statements that ZEITLIN directed, donors were not aware that they were being solicited by and contributing money towards a PAC that focused on political advocacy rather than a charity that provided direct services.

9. For example, in or about 2018, RICHARD ZEITLIN, the defendant, and the Zeitlin Call Centers were hired by the treasurer of a certain PAC ("PAC Treasurer-1") to make solicitation calls on behalf of one of the above-referenced PACs ("PAC-1"). Recipients of fundraising calls from the Zeitlin Call Centers (*i.e.*, potential donors) reported that calls were being made on behalf of PAC-1 that portrayed the organization as a charity that provided certain direct services, including assisting veterans with medical services and housing, rather than as a PAC that engaged

in political activity. In response to reports from PAC Treasurer-1 about donor complaints, ZEITLIN falsely denied that such calls were being made on behalf of PAC-1. At or around the same time, however, ZEITLIN also acknowledged that calls describing PAC-1 as a charity or direct-services organization would be improper. In response to requests by PAC Treasurer-1 to produce recordings of solicitation calls, ZEITLIN refused to provide any such recordings.

10. Nonetheless, the Zeitlin Call Centers continued to make such misrepresentations at certain times when raising funds for certain PACs from at least in or about 2017 through at least in or about 2020. Based at least in part on the false and misleading representations directed and authorized by ZEITLIN, the Zeitlin Call Centers raised tens of millions of dollars in contributions.

11. Between at least in or about 2017 up to and including in or about 2018, RICHARD ZEITLIN, the defendant, also raised money through the Zeitlin Call Centers for certain PACs knowing that none of the money raised on behalf of those PACs would actually fund the PAC. ZEITLIN agreed with treasurers of certain PACs that one of ZEITLIN's entities ("Zeitlin Entity-2") would pay an advance of approximately $30,000 to certain of their PACs, and in exchange, 100 percent of the money subsequently raised by the Zeitlin Call Centers for those PACs over a specified time period (the "100% Time Periods") would be kept by Zeitlin Entity-2 (the "100% Agreements"). Despite the 100% Agreements, ZEITLIN and the Zeitlin Call Centers continued to make calls during the 100% Time Periods to potential donors on behalf of certain PACs falsely representing that donations would be used by those PACS, when in fact all of the money raised during the 100% Time Periods went to Zeitlin Entity-2 rather than to the organization or drive referenced on the fundraising call.

12. Between at least in or about 2017 up to and including in or about 2020, in order to increase funds raised and profits for the Zeitlin Entities, the Zeitlin Call Centers, with the approval

of RICHARD ZEITLIN, the defendant, falsely represented to potential donors that a "new" or "special" drive was "under way" and that their donation would help support the alleged new or special drive.

13. At various times relevant to this Indictment, RICHARD ZEITLIN, the defendant made multiple attempts to conceal his scheme and avoid attracting scrutiny from the public and investigating agencies relating to the Zeitlin Call Centers, the Zeitlin Entities, and ZEITLIN's scheme to defraud. For example:

a. Between at least in or about 2017 up to and including at least in or about 2020, ZEITLIN created various entities that appeared to provide different types of services to PACs from the Zeitlin Call Centers (*i.e.*, the Zeitlin Entities). In or about 2020, ZEITLIN created new entities to effectively replace certain of the existing Zeitlin Entities (*i.e.*, the New Zeitlin Entities). ZEITLIN selected certain of his employees to act as nominal owners of the New Zeitlin Entities even though ZEITLIN managed and controlled them.

b. As a result of ZEITLIN's efforts, invoices for services provided by the Zeitlin Call Centers listed payments owed by PACs to various of the Zeitlin Entities, rather than one entity. Likewise, publicly available FEC reports for PACs that used the Zeitlin Call Centers listed PAC payments made to multiple Zeitlin Entities rather than to one entity, and the PACs therefore appeared to pay different business rather than one business. In addition, ZEITLIN directed an employee to create fraudulent invoices billing certain PACs at an hourly or per-unit rate when, in truth and in fact, each entity was paid not by the hour, but rather, as part of ZEITLIN's overall collection of a large percentage of the money raised (typically approximately 90 percent).

c. On or about December 8, 2020, while testifying under oath during a deposition in connection with a federal civil matter, ZEITLIN falsely stated, in substance and in

part, that neither he nor employees of the Zeitlin Entities provided input as to the call scripts used by the Zeitlin Call Centers when making telemarketing calls on behalf of PACs. In truth and in fact, ZEITLIN and the employees of the Zeitlin Call Centers frequently provided input on and changed call scripts, including by adding false and misleading statements into the call scripts.

d. On or about March 31, 2022, in a declaration filed under penalty of perjury to a federal judge, ZEITLIN falsely stated that, among other things, he was not associated with and did not direct, supervise, or control certain of the New Zeitlin Entities. In truth and in fact, ZEITLIN controlled all the New Zeitlin Entities throughout their existence by exercising ultimate authority over managerial, operational, and financial decisions, including at the time he signed this declaration.

ZEITLIN'S ORDER TO DESTROY RECORDS

14. Beginning in or about 2018 to the present, RICHARD ZEITLIN, the defendant, has maintained a practice of principally communicating with employees of the Zeitlin Call Centers by phone or by encrypted messaging applications that typically delete data after a specified time period, or communicating with employees indirectly through an intermediary. For example, in or about 2018, ZEITLIN, directed certain employees of the Zeitlin Entities to delete materials and documents bearing ZEITLIN's name. In addition, ZEITLIN regularly received information about the operations of the business from CC-1 and relayed messages to others through CC-1.

15. On or about May 24, 2022, in connection with a federal investigation, law enforcement officers served federal grand jury subpoenas to certain individuals associated with the Zeitlin Entities and the PACs for which they solicited donations. On or about the same date, RICHARD ZEITLIN, the defendant, learned about the federal subpoenas and instructed CC-1 to delete his communications on a particularly electronic messaging application ("Application-1")

that Zeitlin's employees used internally to communicate with one another. ZEITLIN also instructed CC-1 to direct other of Zeitlin's employees to do the same. CC-1 relayed ZEITLIN's instruction to certain of Zeitlin's employees. The electronic messages that ZEITLIN instructed his employees to destroy contained internal communications among Zeitlin's employees about the Zeitlin Call Centers and the operations of the Zeitlin Entities, among other things.

STATUTORY ALLEGATIONS

COUNT ONE
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

16. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

17. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343, and did engage in the foregoing in connection with the conduct of telemarketing.

18. It was a part and an object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, ZEITLIN agreed with one or more others to engage in a scheme

to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1349 and 2326.)

COUNT TWO
(Wire Fraud)

The Grand Jury further charges:

19. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

20. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, ZEITLIN engaged in a scheme to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1343, 2326, and 2.)

COUNT THREE
(Conspiracy to Obstruct Justice)

The Grand Jury further charges:

21. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

22. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to obstruct justice, in violation of Title 18, United States Code, Section 1512(c).

23. It was a part and object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, would and did corruptly alter, destroy, mutilate, and conceal a record, document, and other object, and attempt to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise would and did corruptly obstruct, influence, and impede an official proceeding, and attempt to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Section 1512(c) and (k).)

COUNT FOUR
(Obstruction of Justice)

The Grand Jury further charges:

24. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

25. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, corruptly altered, destroyed, mutilated, and concealed a record, document, and other object, and attempted to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise corruptly obstructed, influenced, and impeded an official proceeding, and attempted to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Sections 1512(c) and 2.)

FORFEITURE ALLEGATION

26. As a result of committing the offenses alleged in Counts One and Two of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(8) and 2328, any and all real or personal property used or intended to be used to commit, to facilitate, or to promote the commission of said offenses; and any and all real or personal property constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of said offenses including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses, and any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offenses.

27. As a result of committing the offenses alleged in Counts Three and Four of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28 United States Code, Section 2461(c),

any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

28. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982 and 2328;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

FOREPERSON

DAMIAN WILLIAMS
United States Attorney

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
7815 WEST LA MADRE WAY,
LAS VEGAS, NEVADA 89149

Case No. 2:23-MJ- 744 -VCF

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

See Attachment A-1

I hereby attest and certify on 8/16/23 that the foregoing document is a full, true and correct copy of the original on file in my office, and in my legal custody.
CLERK, U.S. DISTRICT COURT, DISTRICT OF NEVADA
BY: _____ Deputy Clerk

The search and seizure are related to violation(s) of *(insert statutory citations)*:

(1) 18 U.S.C. §§ 1349 and 2326 (conspiracy to commit wire fraud); (2) 18 U.S.C. §§ 1343, 2326, and 2 (wire fraud); (3) 18 U.S.C. § 1512(c), (k) (conspiracy to obstruct justice); and (4) 18 U.S.C. § 1512(c) (obstruction of justice)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-1

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA
Deputy
Secretary

YOU ARE COMMANDED to execute this warrant on or before August 30, 2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/16/23 11:30AM

CAM FERENBACH
Judge's signature

City and state: Las Vegas, Nevada

Hon. Cam Ferenbach
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

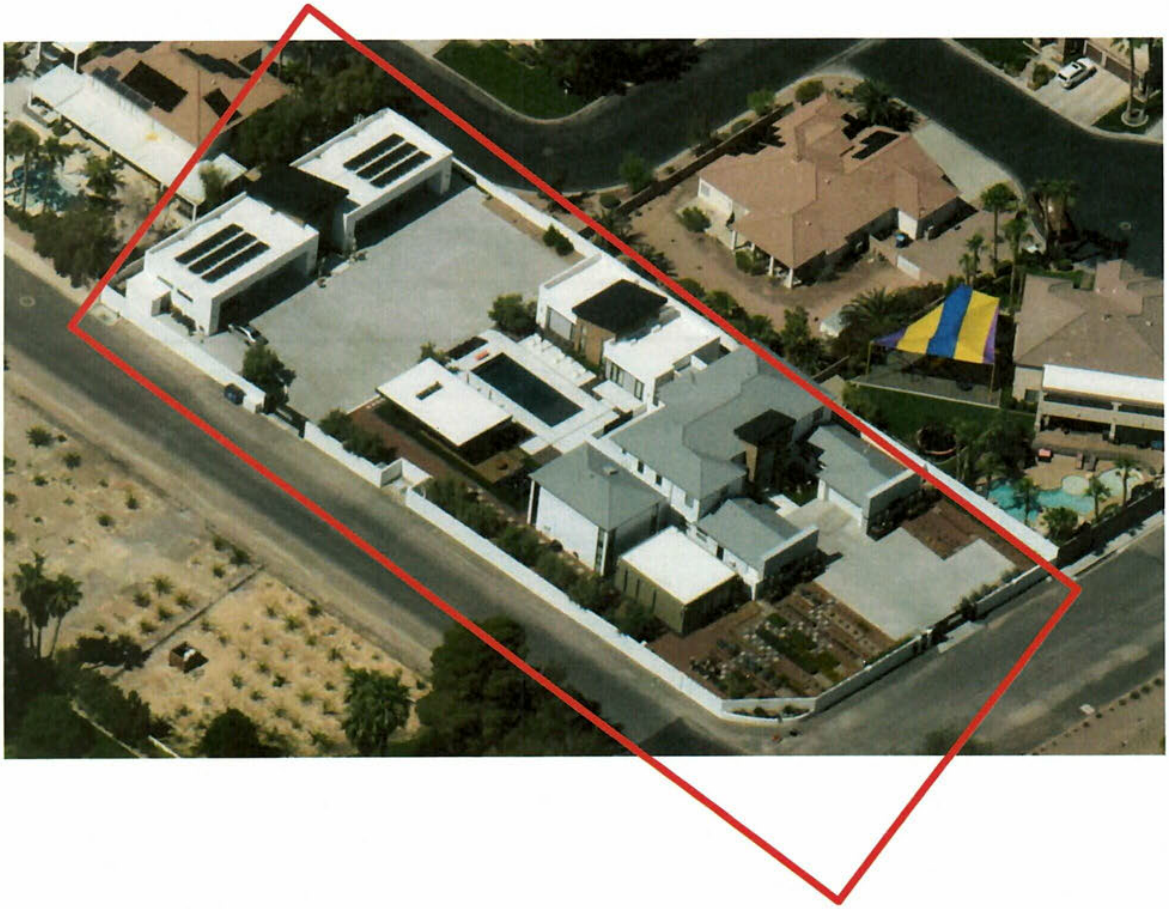
ATTACHMENT A-1

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 7815 West La Madre Way, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-1"), particularly described as a residential property that is surrounded by a solid white wall, with the numbers "7815" facing La Madre Way, and a black or dark grey gate. Inside the wall is a residence that is approximately 9,257 square feet. The residence's exterior is white, with accents and structures that are black, tan, and grey.

An image of the outside of Subject Premises-1 is below:

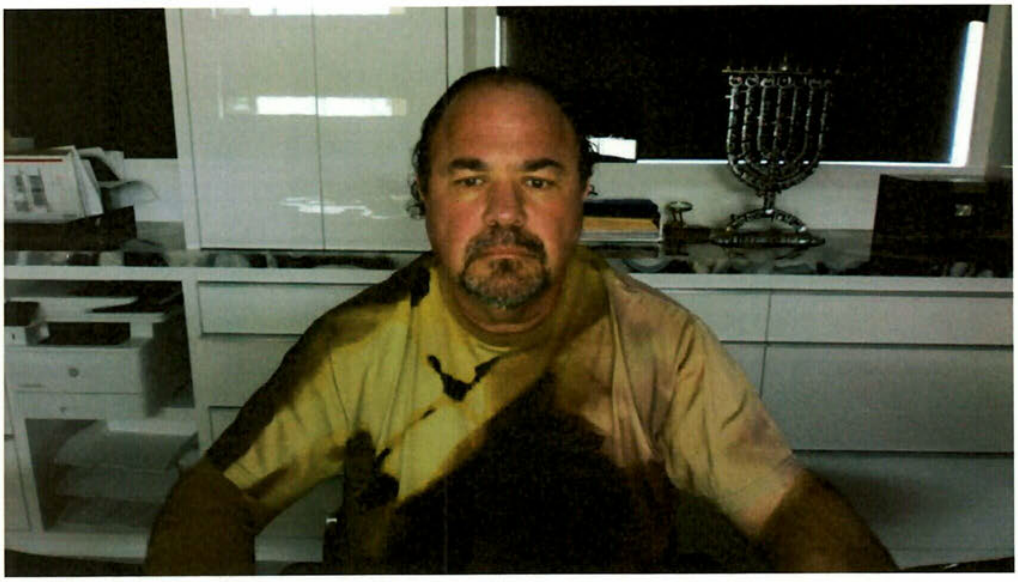
An image of an aerial view of Subject Premises-1 is below, with Subject Premises-1 highlighted with a red box:

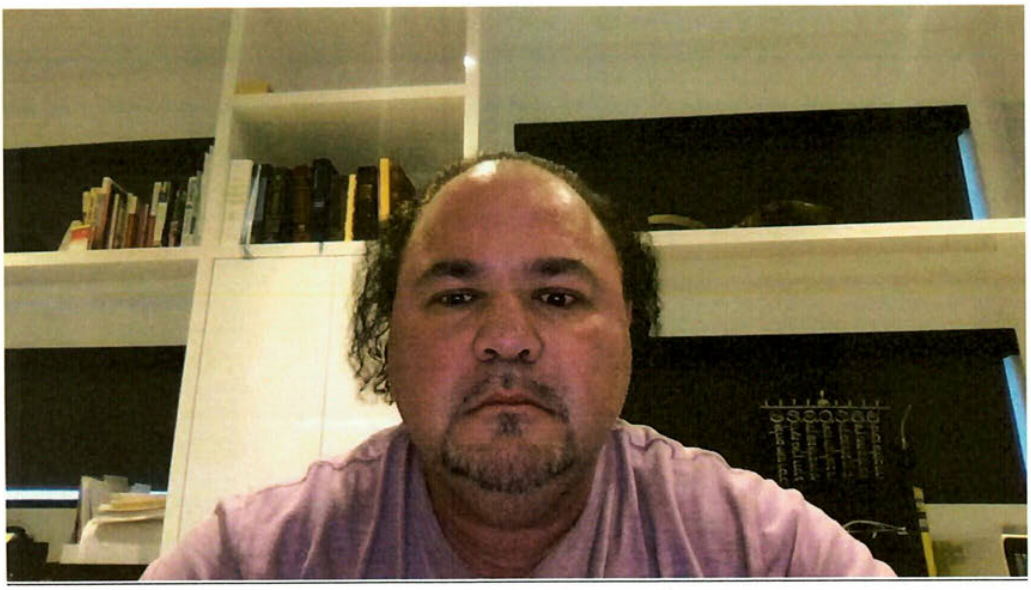


The search of Subject Premises-1 shall include any and all attachments, storage units, casitas, pool houses, and appurtenances thereto, and all other areas within the curtilage. The search of Subject Premises-1 shall also include a search of any and all containers, locked containers, clothing, and personal items (*e.g.*, safes, electronic devices, backpacks, wallets, briefcases, and bags) within Subject Premises-1 at the time of the execution of the search warrant.

The search of Subject Premises-1 shall also include a search of the person of Richard Zeitlin, who was born on November 11, 1970, provided he is located at Subject Premises-1, specifically for the items listed in Attachment B. The search shall not include a body cavity or strip search of any person in the Subject Premises.

Two photographs of Richard Zeitlin are below:





ATTACHMENT B-1

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-1

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-1 by Richard Zeitlin, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to Zeitlin's call center business and its operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among Subjects, co-conspirators, witnesses, current and former clients, and current and former employees and/or associates, including but not limited to communications, photographs and evidence regarding their social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACs, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appear to have been used by Zeitlin and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin, including Apple electronic devices.

v. Any and all electronic devices associated with or that appear to be associated with the phone number 702-247-3310.

w. Any and all electronic devices associated with or that appear to be associated with either or both of the following email addresses: "ccirickz@gmail.com" and/or "rickz@advancedtci.com".

x. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of Nevada

FILED
AUG 16 2023
U.S. MAGISTRATE JUDGE
BY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1835 EAST CHARLESTON BOULEVARD, LAS VEGAS, NEVADA 89104

Case No. 2:23-MJ- 743 -VCF

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

1835 EAST CHARLESTON BOULEVARD, LAS VEGAS, NEVADA 89104 (See Attachment A-2)

located in the _____ District of Nevada , there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment B-2

I hereby attest and certify on 8/16/23 that the foregoing document is a full true and correct copy of the original on file in my office, and in my legal custody.

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA
By _____ Deputy Secretary

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343,1349, 2326, 1512(c) & (k), and 2	Conspiracy to commit wire fraud; wire fraud; conspiracy to obstruct justice; obstruction of justice

The application is based on these facts:

See attached Affidavit and Exhibit 1

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Kelsey Palermo
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by LC
~~telephone~~ in person LC *(specify reliable electronic means).*

Date: 08/16/2023

CAM FERENBACH
Judge's signature

City and state: Las Vegas, Nevada

Honorable Cam Ferenbach
Printed name and title

JASON M. FRIERSON
United States Attorney
District of Nevada
Nevada Bar Number 7709
DAVID KIEBLER
Assistant United States Attorney
501 Las Vegas Boulevard South, Suite 1100
Las Vegas, Nevada 89101
Tel: (702) 388-6519
Fax: (702) 388-6418
David.Kiebler@usdoj.gov
Attorneys for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN THE MATTER OF THE SEARCH OF: 7815 WEST LA MADRE WAY, LAS VEGAS, NEVADA 89149	Case No. 2:23-MJ- 744 -VCF **Affidavit in Support of an Application for a Search Warrant** **(Under Seal)**
IN THE MATTER OF THE SEARCH OF: 1835 EAST CHARLESTON BOULEVARD, LAS VEGAS, NEVADA 89104	Case No. 2:23-MJ- 743 -VCF **Affidavit in Support of an Application for a Search Warrant** **(Under Seal)**

I, KELSEY PALERMO, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an application under Federal Rule of Criminal Procedure 41 for warrants to: (a) search a residential property that is located in the District of Nevada and further described in Attachment A-1, which is incorporated by reference herein: 7815 West La Madre Way, Las Vegas, Nevada 89149, located in Clark County, Nevada (hereafter, "**Subject Premises-1**"); (b) seize from **Subject Premises-1** evidence, fruits, and instrumentalities of the subject offenses described below and in Attachment B-1, which is

incorporated by reference herein, including certain electronic devices as described in Attachment B-1; (c) search a business property that is located in the District of Nevada and further described in Attachment A-2, which is incorporated by reference herein: 1835 East Charleston Boulevard, Las Vegas, Nevada 89104, located in Clark County, Nevada (hereafter, "**Subject Premises-2**," and together with Subject Premises-1, the "**Subject Premises**"); and (d) seize evidence, fruits, and instrumentalities of the subject offenses described below and in Attachment B-2, which is incorporated by reference herein, including certain electronic devices also described in Attachment B-2.

2. The Federal Bureau of Investigation ("FBI" or "Investigating Agency") is investigating fraud committed by Richard ZEITLIN and others through ZEITLIN's telemarketing call center business, which provided, and continues to provide, services to certain charities and political action committees ("PACs"). On or about August 15, 2023, a grand jury sitting in the Southern District of New York returned an Indictment (the "Indictment") charging ZEITLIN in three counts with: (1) conspiracy to commit wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1349 and 2326; (2) wire fraud from at least in or about 2017 through at least in or about 2020, in violation of 18 U.S.C. §§ 1343, 2326, and 2; (3) conspiracy to obstruct justice in or about May 2022, in violation of 18 U.S.C. § 1512(c), (k); and (4) obstruction of justice in or about May 2022, in violation of 18 U.S.C. § 1512(c) (together, the "Subject Offenses"). A copy of the Indictment is attached hereto as Exhibit 1 and is incorporated by reference herein. **Subject Premises-1** is ZEITLIN's residence, and **Subject Premises-2** is one of ZEITLIN's business locations. Based upon the investigation and as set forth in detail below, probable cause exists to believe that the **Subject Premises** contain evidence, fruits, and instrumentalities of the Subject Offenses.

AGENT BACKGROUND

3. I am a Special Agent with the FBI. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the FBI for approximately eight years, and for three years before that I worked as a Staff Operations Specialist with the FBI. For more than one year, I have been assigned to a public corruption squad in the FBI's New York field office. Prior to the FBI's public corruption squad, I was assigned to an FBI counter-intelligence squad. As an FBI Special Agent, I have participated in numerous investigations involving public corruption offenses and fraud, including telemarketing fraud and wire fraud offenses. I have also participated in the execution of search warrants involving premises and electronic evidence. Through my training, education, and experience, I am familiar with the techniques and methods of operation commonly used by individuals engaged in fraud to communicate, operate their scheme(s), conceal their criminal activities, and avoid detection by law enforcement. I am also familiar with the means and methods commonly used by individuals who obstruct justice, including by destroying or deleting evidence and/or directing others to destroy or delete evidence.

4. As an FBI Special Agent, I have received training in the enforcement of federal laws pertaining to public corruption and fraud offenses, including: (1) debriefing defendants, witnesses, and informants, as well as others who have knowledge of public corruption offenses, obstruction offenses, and schemes to defraud, including wire fraud, telemarketing fraud, and frauds that involve PACs; (2) the planning, participation, and/or management of field operations such as surveillance, arrests, the interception of wire communications, and the execution of search warrants; (3) the acquisition, preservation, processing, and analysis of evidence; (4) the

seizure, search, and analysis of electronic devices and electronically stored information; and (5) the tracking of crime proceeds.

5. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. Unless explicitly stated otherwise, all descriptions of conversations are non-verbatim. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

TECHNICAL TERMS

6. Based on my training and experience, and information acquired from other law enforcement officials with technical experience, I know the terms described below have the following meanings:

a. "Electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, external hard drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

b. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually

contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Wireless telephones typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions. Tablets also contain apps.

d. A "storage medium" is any physical object upon which electronic data can be recorded. Examples include USB flash drives, hard disks, RAM, flash memory, CD-ROMs, and other magnetic or optical media.

e. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user

driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

i. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

j. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

k. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of

an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

l. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

m. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

n. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

PROBABLE CAUSE

THE SUBJECT OFFENSES

7. As set forth above, on or about August 15, 2023, a grand jury sitting in the Southern District of New York returned the Indictment, charging ZEITLIN with the Subject Offenses. The Indictment is incorporated by reference herein.

8. As set forth in the Indictment:

a. PACs are entities registered with the Federal Election Commission ("FEC") that may be tax-exempt, and collect money to advocate on behalf of or against certain causes and political candidates. By contrast, charities, unlike PACs, typically provide direct services to communities or causes. Under federal law, independent expenditure-only PACs may raise unlimited contributions provided they do not make expenditures in coordination or in concert with any candidate for federal office or such a candidate's committee. PACs are required to file periodic reports with the FEC providing information about their fundraising and expenditures. Based on these reports, the FEC provides information about each PAC to the public through a searchable public database that shows, among other things, how much money is raised and spent by each PAC and how that money is spent. (Indictment ¶ 3).

b. ZEITLIN has controlled and operated telemarketing call centers (the "Zeitlin Call Centers") for decades, including from at least in or about 1994 to in or about 2023. The Zeitlin Call Centers have raised at least approximately hundreds of millions of dollars for charities and PACs through at least approximately hundreds of thousands of calls to donors and potential donors and various entities that ZEITLIN controlled (the "Zeitlin Entities"). (*Id.* ¶ 1).

c. Initially, the Zeitlin Call Centers provided telemarketing services principally to charities. In or about 2017, however, ZEITLIN decided to shift the business focus of the Zeitlin Call Centers from charity clients to PAC clients. As part of that shift, ZEITLIN

encouraged certain prospective clients to operate PACs rather than charities. ZEITLIN transitioned to servicing primarily PACs in part to avoid certain regulations for charities and requirements associated with telemarketing for charities that do not apply to PACs. (*Id.* ¶ 5).

d. From at least in or about 2017 through at least in or about 2020, ZEITLIN used the Zeitlin Call Centers to defraud numerous donors and potential donors by providing misleading and false information about how the donors' money would be spent and the nature of the organizations to which they were giving. For example, ZEITLIN directed his employees to make calls on behalf of certain PACs that falsely portrayed the PAC as a charity and/or a direct-services organization rather than as a PAC. Even after receiving complaints that the Zeitlin Call Centers were providing false and misleading information to donors and potential donors during fundraising calls, ZEITLIN continued his fraudulent scheme and made efforts to conceal it. The Zeitlin Entities profited from ZEITLIN's fraud, typically keeping a large portion of each dollar donated—approximately 90 percent—the rest of which was disbursed to the respective PAC. (*Id.* ¶ 1).

e. For a period between in or about 2017 and 2018, ZEITLIN entered into agreements with the owner of two PACs to give those PACs a $30,000 advance in exchange for keeping 100% of the money he raised, notwithstanding the fact that ZEITLIN represented to donors during this period that their contributions would help the PAC. (*Id.* ¶ 11).

f. In or about May 2022, after learning that he and the Zeitlin Entities were under federal investigation, ZEITLIN directed at least one of his employees ("CC-1") to instruct other employees of the Zeitlin Entities to delete electronic messages relating to the Zeitlin Call Centers and the operation of the Zeitlin Entities. (*Id.* ¶ 2).

9. Based on my participation in this investigation, including my participation in interviews of former and current ZEITLIN employees, and my review of documents and records, I know the following, among other things:

a. In or about 1994, ZEITLIN created a particular entity for his call center business called Courtesy Call. ZEITLIN has since replaced Courtesy Call and created numerous additional entities (the "Zeitlin Entities") in connection with his call center business. In or about 2020, ZEITLIN replaced his existing entities and created new entities (the "New Zeitlin Entities") in connection with his call center business, enlisting employees and associates to act as the owners of the New Zeitlin Entities even though ZEITLIN continued to direct, supervise, and control them.

b. The Zeitlin Entities and New Zeitlin Entities include, among others: Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. ZEITLIN had pre-existing relationships with certain of his PAC clients. For example, he is close friends with an individual who is the owner/treasurer of at least approximately three PACs that used the Zeitlin Call Centers to raise funds (*i.e.*, ZEITLIN was the best man at his wedding and is the godfather of his child).

d. ZEITLIN is believed to have compensated certain of his employees in a manner that does not immediately appear to be commensurate with their education and experience, at least in part to secure their reliance on ZEITLIN with respect to their livelihood.

THE SUBJECT PREMISES

10. Based on my training and experience, I know that when an individual participates in a criminal scheme, including a scheme to defraud, that individual often maintains documentary evidence of the scheme in their home, including photographs evidencing their relationship with co-conspirators, witnesses, or associates; financial records showing transactions that are evidence of criminal conduct; and business records, including original records, relating to the creation, operation, ownership, development, control, and dissolution of entities used or related to the scheme. I also know that such documentary evidence is frequently stored on electronic devices such as laptop computers, desktop computers, or other electronic storage devices. I also submit there is probable cause that Subject Premises-1 will contain hard-copy and original financial and business records, such as documents establishing certain business entities and bank statements evidencing relevant transactions, as well as electronic files and copies of financial and business records and communications between ZEITLIN and co-conspirators and witnesses, which are likely stored on electronic devices found in or on Subject Premises-1.

11. Based on my training and experience, I know that senior executives, senior managers, and owners of businesses commonly work from home and/or have home offices because of the nature of their roles and responsibilities, which typically require the individual to work after-hours and on the weekends, the need to access certain business and financial documents after-hours in order to operate and manage their businesses, the need to protect certain important, confidential, or sensitive business and financial records, the individual's ability to more freely determine from where he or she will work (*i.e.*, when they will work remotely), the increased frequency and/or necessity of business travel for the individual because of his or her role (and thus the need to carry more work-related materials home), and the increased frequency of personal travel for the individual because he or she may have the resources and flexibility to

do so. I also know that following the COVID-19 pandemic's height in or about early 2020, many Americans began working more frequently from home or remotely. As a result, senior executives, managers, and owners of businesses commonly possess and retain business-related documents within their homes.

12. Based on my training and experience, I know the following, in substance and in part, concerning the use of electronic devices and electronic evidence in criminal schemes:

a. Individuals engaged in fraud typically utilize electronic equipment such as computers, software programs, cellular telephones, mobile applications, and other electronic devices to further facilitate their illicit scheme.

b. Individuals who participate in criminal schemes, such as schemes to defraud and schemes to destroy evidence, commonly use electronic communications to communicate with co-conspirators, establish and use online financial accounts, keep track of co-conspirator information; and keep a record of illegal transactions or criminal proceeds for future reference.

c. When an individual participates in a criminal scheme, photographs or videos stored in that individual's cellphone(s) and other electronic devices often contain evidence of that scheme because such photographs or videos can provide evidence of relationships between participants in the scheme and the time and/or location of meetings between co-conspirators.

d. When an individual participates in a criminal scheme, that individual's web browser history often contains evidence of that scheme. For example, individuals who engage in schemes to defraud who seek to avoid law enforcement detection may conduct research on relevant legal rules and regulations. Here, for instance, ZEITLIN may have conducted research on FEC regulations, telemarketing regulations, PAC regulations, charity regulations, and state and federal laws pertaining to telemarketing and fraud. Likewise, individuals who engage in

methods to avoid law enforcement detection—including, for example, by reducing electronic communications or communicating through encrypted applications—may have conducted research on encryption, applications and devices that encrypt communications, and applications that do not save or store data. Finally, individuals who seek to destroy evidence may research technical mechanisms to permanently delete electronic evidence so that it may not be recovered.

e. Historical location data collected by a user's cellphone(s) and other electronic devices can be relevant to establishing that user's participation in a criminal conspiracy, such as by showing when the relevant actors were together in person and thus how and when information was transmitted.

f. Individuals who engage in criminal schemes commonly maintain electronic records relating to their schemes, such as contact information for co-conspirators, records of illegal transactions or criminal proceeds, and financial account statements. These materials can be easily moved between an individual's electronic devices and storage accounts, such as by email and file sharing and transfers between devices and accounts.

g. Electronic communications platforms, like email, text messages, and Signal, can often be accessed from multiple devices like a user's mobile devices and desktop computer. Based on my interviews with several Zeitlin Call Center employees, I know that Zeitlin communicated with his employees through Signal and occasionally through email. Based on my review of publicly available information, I know that a single Signal account can be accessed from a mobile device and desktop computer.[1]

[1] *See Installing Signal*, Signal.com, https://support.signal.org/hc/en-us/articles/360008216551-Installing-Signal ("You can link Signal Desktop to your mobile device to send and receive Signal messages from your laptop or desktop computer.").

h. Where electronic messages or other electronic files are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because electronic files can be stored on cellphones or other electronic devices or computer servers for years at little or no cost and users thus may have little incentive to delete data that may be useful to consult in the future.

13. Based on my training and experience, I know that cellphones are frequently kept at the owner's residence and/or on their owner's person where the owner has immediately access to them. I also know that individuals who own cellphones often backup or sync the data on those cellphones to other electronic devices such as laptop computers, desktop computers, or other electronic storage devices.

14. Based on my training and experience and my participation in this investigation, I know that even individuals who have destroyed or have attempted to destroy evidence, and individuals who attempt to evade law enforcement detection by reducing the use of non-encrypted communications, may not know what evidence is relevant or important to law enforcement and how to permanently delete evidence.

Subject Premises-1

15. I believe that ZEITLIN resides at **Subject Premises-1** based on the following, among other things:

a. Based on my review of publicly available information, including records from an online business portal provided by the Nevada Secretary of State ("SilverFlume"), I know that Unified Data Services LLC, one of the Zeitlin Entities, was formed on or about August 15, 2018, and listed ZEITLIN as a "Manager" with **Subject Premises-1** as ZEITLIN's address.

b. On or about April 18, 2023, the Honorable Jennifer E. Willis, U.S. Magistrate Judge, Southern District of New York, issued a warrant (the "SCA Warrant") for all

content and other information associated with the Google Account with email address "ccirickz@gmail.com," an account believed to be used by ZEITLIN ("Zeitlin Email-1").[2] Based on my review of emails and records produced by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, my participation in this investigation, and my conversations with other law enforcement officers, I know the following, among other things:

i. On or about January 30, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Mon, Jan 30," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject Premises-1**, including an envelope from a P.O. Box in San Antonio, Texas; a tax document from one of the New Zeitlin Entities, "LAV Services LLC," in Cedar City, Utah; and a "Pre-Paid Service Notice" for "Heating System Check" and "Water Heater Inspection and Flush" addressed to "Rick & Luliana [sic] Zeitlan [sic]" (all caps in the original). I believe "Liliana Zeitlin" is the name of ZEITLIN's current or former spouse, from whom ZEITLIN is either separated or divorced.[3]

ii. On or about March 15, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Wed, Mar 15," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject**

[2] The SCA Warrant authorized the search of records associated with several email addresses, including Zeitlin Email-1 and a second email address used be Zeitlin, "rickz@advancedtci.com" ("Zeitlin Email-2").

[3] This email also included images of tax documents addressed to "Jordan Zeitlin" at **Subject Premises-1** (all caps in the original) and Sarah H Zeitlin" at **Subject Premises-1** (all caps in the original).

Premises-1, including an envelope marked "Reservations" and "Personal and Confidential" (all caps in the original).[4]

iii. On or about April 5, 2023, ZEITLIN received an email from the U.S. Postal Service with subject line "Your Daily Digest for Wed, Apr 5," informing ZEITLIN that certain items would be "coming to your mailbox soon" (all caps in the original). The email included images of various mailings that were addressed to "Richard Zeitlin" at **Subject Premises-1**, including an envelope from SiriusXM, an envelope from Charles Schwab, an envelope from Capital Bank, and two envelopes from Las Vegas Valley Water District (addressed to "Zeitlin, Liliana" and "Zeitlin, Richard L").

16. Based on my review of records provided by the U.S. Postal Service, my participation in this investigation, and my conversations with other law enforcement officers, I know, among other things, that on or about July 12, 2023, U.S. mail addressed to ZEITLIN on behalf of "Advance Telephony LLC," one of the Zeitlin Entities, was delivered to **Subject Premises-1**. I believed "Advance Telephony LLC" is a reference to Advanced Telephony Consultants, one of the Zeitlin Entities set forth above.[5]

17. On or about August 10, 2023, the Honorable Gabriel W. Gorenstein, U.S. District Judge, Southern District of New York, issued a warrant (the "GPS Warrant") for prospective and historical location information and pen register information for the cellphone assigned call

---

[4] The email also included images of two tax documents enclosed with a perforated seal from "LAV SERVICES LLC" addressed to "Sheryl Teller" at "615 Crescent Lane" in "Thiensville WI." Based on my review of law enforcement databases, I understand that "Sheryl Teller" has previously used the last name "Zeitlin," and accordingly may be a relative of ZEITLIN. The recipient name and address on these tax documents (*i.e.*, the name Sheryl Teller" and the address below) is typed in a different font and size than the recipient name and address on the tax documents referenced above, and appears to have been typed and printed and affixed to these documents on top of the original recipient name and address.

[5] Based on my participation in this investigation, I also know that ZEITLIN owns other properties, including a residence in Mexico.

number 702-241-3310, a phone number subscribed in the name of Richard Zeitlin and believed to be used by ZEITLIN ("Zeitlin Phone-1").

a. Based on data and information provided by Verizon Wireless, as of the evening of on or about August 13, 2023, Zeitlin Phone-1 was located in the vicinity of **Subject Premises-1**.

18. Based on my review of documents and records provided by Apple in or about August 2023, I know that as of in or about August 2023, several Apple electronic devices were associated with Zeitlin Phone-1. These devices were activated between in or about May 2010 through in or about March 2023, and include Apple iPhones, iPads, iPods, TVs, iMac desktop computers, and Macbook laptops.

19. As discussed above, I know that owners, senior executives, and senior managers of businesses often work remotely and/or work from home. Based on my participation in this investigation, including my participation in interviews of [redacted], I know that ZEITLIN regularly conducted business by phone—that is, from outside of a business office—in addition to, at times, meeting in person with certain Zeitlin employees, including at **Subject Premises-2** and an office in the Whitney Ranch neighborhood of Henderson, Nevada (the "Whitney Ranch Office"). ZEITLIN communicated with

[redacted]

employees, principally CC-1, by phone or encrypted messaging application. I also know that many of Zeitlin's employees also worked remotely and/or from home.

20. Based on my review of a page on Zillow.com, a website that shows current and historical real estate listings, I have reviewed a real estate posting for **Subject Premises-1**, which included several photographs of what I believe to be **Subject Premises-1**.[7] One of the photographs, shown below, appears to show a home office inside **Subject Premises-1**:

The photograph above has a mark in the bottom left part of the screen that says "LVR 2022," which, based on my training and experience, shows that the photograph was created in or about 2022.[8]

[7] *See* 7815 W La Madre Way, Las Vegas, NV 89149, Zillow, https://www.zillow.com/homedetails/7815-W-La-Madre-Way-Las-Vegas-NV-89149/6900730_zpid/ (last visited Aug. 11, 2023).

[8] Attachment A-1 includes two photographs of ZEITLIN that that were included in grand jury subpoena returns for a financial account controlled by ZEITLIN. The two photographs of ZEITLIN in Attachment A-1 appear to show ZEITLIN seated at the desk shown in the above photograph of **Subject Premises-1**, based on my review of the three photographs.

21. Based on my review of data and records provided by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, I have learned that ZEITLIN has had the following online activity, among other activity:

a. On or about April 3, 2023, ZEITLIN accessed the website for Wells Fargo, a national bank.

b. On or about April 2, 2023, ZEITLIN visited a webpage titled "Leaving the US While Indicted" using a Google Chrome web browser.

c. On or about March 16, 2023, ZEITLIN visited the website for Citibank, a national bank.

d. On or about March 14, 2023, ZEITLIN accessed an email in his Google email account with the subject line "FEC hotline number."

e. On or about March 9, 2023, ZEITLIN visited webpages on the FEC website titled "FEC | Nonconnected | Notices required on PAC solicitations" and "Nonconnected committee webstore/fundraiser disclaimer example."

f. On or about March 8, 2023, ZEITLIN visited a webpage on the FEC website titled "FEC | Nonconnected | Notices required on PAC solicitations" and search on Google for the phrase "notices required on non connected pac solicitations."

22. Based on the foregoing, I believe there is probable cause to believe that **Subject Premises-1** will contain evidence, fruits, and instrumentalities of the Subject Offenses, including electronic devices.

Subject Premises-2

23. I know **Subject Premises-2** continues to be used by employees of the Zeitlin Call Centers to conduct the work of the Zeitlin Call Centers for the following reasons, among others:

a. Based on my participation in this investigation and my review of a transcript of a deposition of ZEITLIN in connection with a federal civil lawsuit, I know that on or about December 8, 2020, ZEITLIN stated the following, in substance and in part, under oath:

i. ZEITLIN owns a real estate company called "MRZ Management" that manages approximately two properties: **Subject Premises-2** and a property at 1009 Whitney Ranch Drive in Henderson, Nevada (*i.e.*, the Whitney Ranch Office, referenced above).

ii. Courtesy Call, the entity associated with the Zeitlin Call Centers, and Donor Relations, another entity associated with the Zeitlin Call Centers, were headquartered at **Subject Premises-2** up until in or about 2018. As of in or about 2020, a company that ZEITLIN partially owns, Chrome Builders Construction, formally operated out of **Subject Premises-2**.

b. Based on my participation in this investigation, including my participation in interviews of [redacted] I know that **Subject Premises-2** is commonly referred to as the "Charleston" office because it is located on Charleston Boulevard

c. Based on my review of electronic messages provided to the Government in response to a grand jury subpoena, I know that on or about June 15, 2022, an employee of the Zeitlin Call Centers ("Employee-1") communicated with an individual who provides IT services to the Zeitlin Call Centers (*i.e.*, Employee-2) about **Subject Premises-2** via a communications application called Skype. Specifically, Employee-1 wrote to Employee-2 that two other employees ("Employee-3" and "Employee-4") needed office space at **Subject Premises-2**. Employee-1 and Employee-2 had the following exchange:

> Employee-1: [Employee-3] and [Employee-4] need an office at Charleston [*i.e.*, **Subject Premises-2**] to work in so he can teach her how to help him with scripting. It will take at least a month, maybe 2. Is anything available there?

Employee-2: yes/no lol

Employee-2: do they need a quiet place?

Employee-2: or will they be ok in a big open room

Employee-2: we were going to stick the couple people in the big open IT area []

. . .

Employee-1: It should work, they won't be recording, just putting everything together.

Employee-2: ok that was the plan was to put 4 desks in chrome… One for ["Employee-5"] and one for ["Employee-6"] and 2 for whatever else

Employee-2: looks like movers will be at the office on the 24th…

Employee-2: so need to make sure everyone has packed all their personal shit and gotten it out of there

Employee-1: What's a good date to tell [Employee-3's first name] and [Employee-4's first name] they can start at Charleston?

Employee-2: lets get through this move first cuz [sic] I have to find/source build 2 computers for them it will be fun

Employee-1: They were just going to move their computers from home to the office and then back when done. Just need a place to set it up.

Employee-2: ohh in that case the week after we move should be perfectly fine

Employee-2: ill [sic] make sure there is a power strip and a hot network cable for them

Based on my participation in this investigation and my conversations with other law enforcement officers, when Employee-2 wrote that "the plan was to put 4 desks in chrome," I understand Employee-2 was communicating, in substance and in part, that **Subject Premises-2** is the formal

office space for ZEITLIN's business, Chrome Builders Construction (*i.e.*, "chrome"), but Employee-2 was planning to put four desks in **Subject Premises-2** that employees of the Zeitlin Call Centers could use.[9]

[redacted]

[9] I am not aware of any evidence suggesting that Employee-1, Employee-2, or Employee-3 have done any work for Chrome Builders Construction.

[redacted]

18 _____

19 10 [redacted]

20 11 [redacted]

21

22

23

24

24. Based on my review of records provided by Google pursuant to the SCA Warrant and relating to Zeitlin Email-1, I have learned that Zeitlin had the following online activity, among other activity: On or about February 21, 2023, Zeitlin searched for, among others, the phrases: "1835 e charleston blvd las vegas assesors," "1835 e charleston blvd las vegas," and "clark county assessor 1835 E." Each of these searches references the address for **Subject Premises-2**.

25. Based on my experience and training and my participation in this investigation, I know that the vast majority of businesses use electronic devices, including computers. Here, I know that employees of the Zeitlin Call Centers regularly used electronic devices in their work and that call centers scripts and recordings were created, edited, shared, and circulated electronically. I also know that when employees of a business and/or entity, such as the Zeitlin Call Centers, continue to use an office space, desk, or workspace, formally or informally, work relating to that business or entity, including the work of those employees, typically remains at that office space.

26. Based on the foregoing, I believe there is probable cause to believe that **Subject Premises-2** will contain evidence, fruits, and instrumentalities of the Subject Offenses, including electronic devices.

SEIZURE OF ELECTRONIC DEVICES

27. As described above and in Attachments A-1, A-2, B-1, and B-2, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information

[redacted]

that might be found at the **Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on electronic devices. Thus, the applied-for warrant would authorize the search of the **Subject Premises**, as described in Attachment A-1 and A-2 to this Affidavit and to the Search Warrant, for the items described in Attachment B-1 and B-2 to this Affidavit and to the Search Warrant, including the seizure of electronic devices believed to be used by ZEITLIN and/or by employees and/or associates of the Zeitlin Entities and/or the Zeitlin Call Centers, including computers, cellphones, and electronic storage media, and potentially, the copying of such electronic devices and electronically stored information ("ESI"), under Rule 41(e)(2)(B).

28. Based on my training and experience and my participation in this investigation, including my review of the evidence gathered in this investigation, my review of data, reports, and records, my participation in interviews of witnesses, and my conversations with other law enforcement officers, and for the reasons set forth in this Affidavit, I submit that if an electronic device is found at the **Subject Premises**, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the Subject Offenses will be found on those electronic devices.

29. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic

storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

30. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any electronic devices, including computer devices, storage media, and cellphones, or potentially copy such electronic devices, and then transport the seized electronic devices to the Southern District of New York as described further below. The seizure of the electronic device is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

31. **Subject Premises-1** is a residence at which individuals other than ZEITLIN may reside. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on scene which electronic devices have been and/or are used by

ZEITLIN and which electronic devices have not been used by ZEITLIN, for example, based on the location of the device.

32. **Subject Premises-2** is a business location at which employees of ZEITLIN and the Zeitlin Call Centers have worked and are believed to continue to work. As discussed herein, the Zeitlin Call Centers (the "Company"), which is associated with numerous business entities, appears to be a functioning company that conducts some legitimate business. The seizure of the Company's computers or other storage media may limit the Company's ability to conduct its legitimate business. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on the scene what computers or storage media have been used by ZEITLIN and/or associates and/or employees of ZEITLIN in connection with the Zeitlin Call Centers and/or the Zeitlin Entities, as well as what electronic devices must be seized or may be copied, based on the location of the electronic devices, materials surrounding the electronic devices, and any markings on the electronic devices. Law enforcement personnel may speak with Company personnel on the scene as may be appropriate to determine the user(s) of the electronic devices. Where appropriate, law enforcement personnel will copy data, rather than physically seize computers, to reduce the extent of any disruption of the Company's business operations. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continued functioning of the Company's legitimate business. If, after inspecting the seized computers off-site, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the Government will return it.

33. Following seizure of any electronic devices, including cellphones, computer devices, and storage media from the **Subject Premises** and/or the creation of forensic image copies, the FBI intends to transport the electronic devices to the Southern District of New York

and seek judicial authority to search any electronically stored information contained therein for evidence of the Subject Offenses.

CONCLUSION

34. I respectfully submit that this affidavit supports probable cause to search the **Subject Premises** as described in Attachment A- and Attachment A-2 to this Affidavit and to the warrants and seize the items listed in Attachment B-1 and Attachment B-2 to this Affidavit and to the warrants, including electronic devices.

35. In light of the confidential nature of this investigation, and the fact that premature disclosure of this Affidavit could alert subjects of the investigation as to the nature and scope of the investigation, thereby prompting them to destroy evidence, shape their testimony, or tamper with witnesses, I respectfully request that the Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise and with the exception of the Government's disclosures pursuant to its discovery and disclosure obligations.

KELSEY PALERMO
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 X by telephone / in person on the 16th day of August, 2023.

CAM FERENBACH
HONORABLE CAM FERENBACH
UNITED STATES MAGISTRATE JUDGE

I hereby attest and certify on 8/16/23 that the foregoing document is a full true and correct copy of the original on file in my office, and in my legal custody.

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEVADA

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

By _____ Deputy Secretary

ATTACHMENT A-1

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 7815 West La Madre Way, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-1"), particularly described as a residential property that is surrounded by a solid white wall, with the numbers "7815" facing La Madre Way, and a black or dark grey gate. Inside the wall is a residence that is approximately 9,257 square feet. The residence's exterior is white, with accents and structures that are black, tan, and grey.

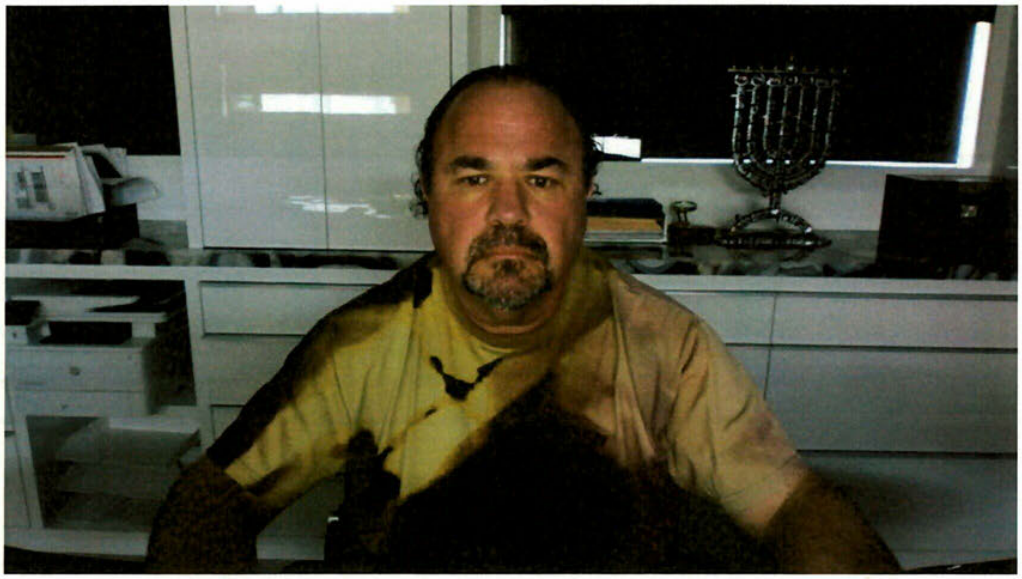
An image of the outside of Subject Premises-1 is below:

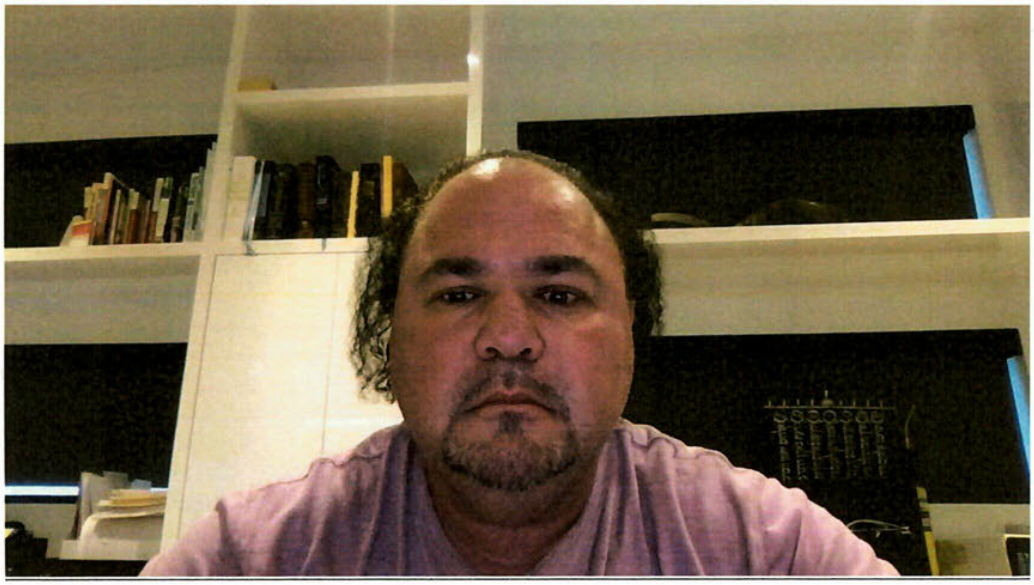
An image of an aerial view of Subject Premises-1 is below, with Subject Premises-1 highlighted with a red box:

The search of Subject Premises-1 shall include any and all attachments, storage units, casitas, pool houses, and appurtenances thereto, and all other areas within the curtilage. The search of Subject Premises-1 shall also include a search of any and all containers, locked containers, clothing, and personal items (*e.g.*, safes, electronic devices, backpacks, wallets, briefcases, and bags) within Subject Premises-1 at the time of the execution of the search warrant.

The search of Subject Premises-1 shall also include a search of the person of Richard Zeitlin, who was born on November 11, 1970, provided he is located at Subject Premises-1, specifically for the items listed in Attachment B. The search shall not include a body cavity or strip search of any person in the Subject Premises.

Two photographs of Richard Zeitlin are below:





ATTACHMENT A-2

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 1835 East Charleston Boulevard, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-2"), particularly described as a commercial property with a reddish-brown brick exterior, windows with white window frames, and a flat white awning that reads "CHARLESTON PROFESSIONAL BUILDING" in dark blue print on the left and "GENERAL CONTRACTOR" in lighter blue print on the right when facing Subject Premises-2. A white rectangular placard with the numbers "1835" in white sits above the white awning and is affixed to a white architectural structure with columns and grating. In front of Subject Premises-2 are approximately six parking spaces for vehicles to park perpendicular to the street in front of Subject Premises-2. The door to Subject Premises-2 is white and below and offset to the left of the portion of the awning that reads "GENERAL CONTRACTOR."

Two images of Subject Premises-2 are below with the white door highlighted with a red circle in the second image below. Subject Premises-2 does not include the orange building depicted in the images below that is to the right of Subject Premises-2 and marked with a placard reflecting a street number of "1837."


1900 E Charleston Blvd
WE FIX PHONES
FOR LEASE
BUILD TO SUIT
3B7 PHONE HOUSE
CHARLESTON PROFESSIONAL BUILDING
GENERAL CONTRACTOR
LIQUIDATION
Google


Las Vegas, Nevada
FOR EASE
IMMEDIAT OCCUPANC
UTILITIES INCLUDED
NO CAMS
BUILD TO SUIT
702 278 1275
CHARLESTON
SSIONAL BUILDING
GEN RAL CONTRACTOR
1837
Google

ATTACHMENT B-1

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-1

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-1 by Richard Zeitlin, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to Zeitlin's call center business and its operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among Subjects, co-conspirators, witnesses, current and former clients, and current and former employees and/or associates, including but not limited to communications, photographs and evidence regarding their social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACs, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appear to have been used by Zeitlin and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin, including Apple electronic devices.

v. Any and all electronic devices associated with or that appear to be associated with the phone number 702-247-3310.

w. Any and all electronic devices associated with or that appear to be associated with either or both of the following email addresses: "ccirickz@gmail.com" and/or "rickz@advancedtci.com".

x. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

ATTACHMENT B-2

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-2

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-2, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Richard Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to call centers associated with and/or operated by Zeitlin and their operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among co-conspirators and witnesses, including but not communications, limited to social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACS, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appears to have been used by Zeitlin and current and former employees and/or associates of Zeitlin, and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin.

v. A black and silver computer monitor and computer tower that is believed to have been used by and/or appears to have been used by a former employee of Zeitlin.

w. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

RICHARD ZEITLIN,

Defendant.

SEALED INDICTMENT

23 Cr. _____ (___)

23 CRIM 419

The Grand Jury charges:

OVERVIEW

1. RICHARD ZEITLIN, the defendant, has controlled and operated telemarketing call centers (the "Zeitlin Call Centers") for decades, including from at least in or about 1994 to in or about 2023. The Zeitlin Call Centers have raised at least approximately hundreds of millions of dollars for charities and political action committees ("PACs") through at least approximately hundreds of thousands of calls to donors and potential donors and various entities that ZEITLIN controlled (the "Zeitlin Entities"). From at least in or about 2017 through at least in or about 2020, ZEITLIN used the Zeitlin Call Centers to defraud numerous donors and potential donors by providing misleading and false information about how the donors' money would be spent and the nature of the organizations to which they were giving. For example, ZEITLIN directed his employees to make calls on behalf of certain PACs that falsely portrayed the PAC as a charity and/or a direct-services organization rather than as a PAC. Even after receiving complaints that the Zeitlin Call Centers were providing false and misleading information to donors and potential donors during fundraising calls, ZEITLIN continued his fraudulent scheme and made efforts to conceal it. The Zeitlin Entities profited from ZEITLIN's fraud, typically keeping a large portion

of each dollar donated—approximately 90 percent—the rest of which was disbursed to the respective PAC.

2. In or about May 2022, after learning that he and the Zeitlin Entities were under federal investigation, RICHARD ZEITLIN, the defendant, directed at least one of his employees ("CC-1") to instruct other employees of the Zeitlin Entities to delete electronic messages relating to the Zeitlin Call Centers and the operation of the Zeitlin Entities.

BACKGROUND

3. PACs are entities registered with the Federal Election Commission ("FEC") that may be tax-exempt, and collect money to advocate on behalf of or against certain causes and political candidates. By contrast, charities, unlike PACs, typically provide direct services to communities or causes. Under federal law, independent expenditure-only PACs may raise unlimited contributions provided they do not make expenditures in coordination or in concert with any candidate for federal office or such a candidate's committee. PACs are required to file periodic reports with the FEC providing information about their fundraising and expenditures. Based on these reports, the FEC provides information about each PAC to the public through a searchable public database that shows, among other things, how much money is raised and spent by each PAC and how that money is spent.

4. RICHARD ZEITLIN, the defendant, has owned and operated telemarketing call centers (*i.e.*, the Zeitlin Call Centers) for decades, beginning in at least in or about 1994 when he created a particular entity ("Zeitlin Entity-1"). After Zeitlin Entity-1, ZEITLIN opened and operated a number of different entities (*i.e.*, the Zeitlin Entities), in connection with the Zeitlin Call Centers. In or about 2020, ZEITLIN effectively replaced certain of the Zeitlin Entities with new entities (together, the "New Zeitlin Entities"), also in connection with the Zeitlin Call Centers.

5. Initially, the Zeitlin Call Centers provided telemarketing services principally to charities. In or about 2017, however, RICHARD ZEITLIN, the defendant, decided to shift the business focus of the Zeitlin Call Centers from charity clients to PAC clients. As part of that shift, ZEITLIN encouraged certain prospective clients to operate PACs rather than charities. ZEITLIN transitioned to servicing primarily PACs in part to avoid certain regulations for charities and requirements associated with telemarketing for charities that do not apply to PACs.

6. The Zeitlin Call Centers employed call center employees or telemarketers in the United States and abroad to call potential donors and solicit financial contributions. These phone calls used either a live call center employee following a written script or pre-recorded portions of a script that a call center employee would play in response to statements made by the potential donor (such as playing, "Can I talk to your mom or dad please?" if a child answered the phone) so that the donor would believe they were having a conversation with a live telemarketer. In either case, PAC treasurers, who were responsible for their respective PACs, were led to believe they had ultimate approval over the call scripts used to solicit contributions. The Zeitlin Entities kept a substantial percentage of the funds raised by the Zeitlin Call Centers—typically approximately 90 percent. The remaining funds went to the charity or PAC on whose behalf the donations were made. As a result of this pay structure, the more funds the Zeitlin Call Centers raised for PACs and charities, the more money the Zeitlin Entities, and thus RICHARD ZEITLIN, the defendant, ultimately made.

ZEITLIN'S SCHEME TO DEFRAUD DONORS

7. From at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, defrauded donors and potential donors by directing employees of the Zeitlin Call Centers to make fundraising calls containing false and/or misleading statements that

misled donors and potential donors into believing that they were donating money (a) to a charity or direct-services organization rather than to a PAC; (b) that would go to an organization (rather than to the telemarketers); and/or (c) to support a "new" or "special" drive that was underway.

8. Specifically, from at least in or about 2017 through at least in or about 2020, RICHARD ZEITLIN, the defendant, directed employees of the Zeitlin Entities to alter the call scripts used when calling potential donors on behalf of certain PACs in order to mislead potential donors into believing that they would be giving to a direct-services organization (*i.e.*, a charity), rather than to a political advocacy organization, (*i.e.*, a PAC). ZEITLIN directed that these lies, misleading statements, and misrepresentations be made so that the donors would be more likely to give money as a result of the call, thereby increasing the funds raised and profits for the Zeitlin Entities. For instance, ZEITLIN directed employees to change call scripts to suggest that the organization soliciting donations performed direct services by, for example, telling a potential donor that "your support helps the handicapped and disabled veterans by working on getting them the medical needs the VA doesn't provide" and/or to remove references to "PAC" or "political action committee." Because of these misleading statements that ZEITLIN directed, donors were not aware that they were being solicited by and contributing money towards a PAC that focused on political advocacy rather than a charity that provided direct services.

9. For example, in or about 2018, RICHARD ZEITLIN, the defendant, and the Zeitlin Call Centers were hired by the treasurer of a certain PAC ("PAC Treasurer-1") to make solicitation calls on behalf of one of the above-referenced PACs ("PAC-1"). Recipients of fundraising calls from the Zeitlin Call Centers (*i.e.*, potential donors) reported that calls were being made on behalf of PAC-1 that portrayed the organization as a charity that provided certain direct services, including assisting veterans with medical services and housing, rather than as a PAC that engaged

in political activity. In response to reports from PAC Treasurer-1 about donor complaints, ZEITLIN falsely denied that such calls were being made on behalf of PAC-1. At or around the same time, however, ZEITLIN also acknowledged that calls describing PAC-1 as a charity or direct-services organization would be improper. In response to requests by PAC Treasurer-1 to produce recordings of solicitation calls, ZEITLIN refused to provide any such recordings.

10. Nonetheless, the Zeitlin Call Centers continued to make such misrepresentations at certain times when raising funds for certain PACs from at least in or about 2017 through at least in or about 2020. Based at least in part on the false and misleading representations directed and authorized by ZEITLIN, the Zeitlin Call Centers raised tens of millions of dollars in contributions.

11. Between at least in or about 2017 up to and including in or about 2018, RICHARD ZEITLIN, the defendant, also raised money through the Zeitlin Call Centers for certain PACs knowing that none of the money raised on behalf of those PACs would actually fund the PAC. ZEITLIN agreed with treasurers of certain PACs that one of ZEITLIN's entities ("Zeitlin Entity-2") would pay an advance of approximately $30,000 to certain of their PACs, and in exchange, 100 percent of the money subsequently raised by the Zeitlin Call Centers for those PACs over a specified time period (the "100% Time Periods") would be kept by Zeitlin Entity-2 (the "100% Agreements"). Despite the 100% Agreements, ZEITLIN and the Zeitlin Call Centers continued to make calls during the 100% Time Periods to potential donors on behalf of certain PACs falsely representing that donations would be used by those PACS, when in fact all of the money raised during the 100% Time Periods went to Zeitlin Entity-2 rather than to the organization or drive referenced on the fundraising call.

12. Between at least in or about 2017 up to and including in or about 2020, in order to increase funds raised and profits for the Zeitlin Entities, the Zeitlin Call Centers, with the approval

of RICHARD ZEITLIN, the defendant, falsely represented to potential donors that a "new" or "special" drive was "under way" and that their donation would help support the alleged new or special drive.

13. At various times relevant to this Indictment, RICHARD ZEITLIN, the defendant made multiple attempts to conceal his scheme and avoid attracting scrutiny from the public and investigating agencies relating to the Zeitlin Call Centers, the Zeitlin Entities, and ZEITLIN's scheme to defraud. For example:

a. Between at least in or about 2017 up to and including at least in or about 2020, ZEITLIN created various entities that appeared to provide different types of services to PACs from the Zeitlin Call Centers (*i.e.*, the Zeitlin Entities). In or about 2020, ZEITLIN created new entities to effectively replace certain of the existing Zeitlin Entities (*i.e.*, the New Zeitlin Entities). ZEITLIN selected certain of his employees to act as nominal owners of the New Zeitlin Entities even though ZEITLIN managed and controlled them.

b. As a result of ZEITLIN's efforts, invoices for services provided by the Zeitlin Call Centers listed payments owed by PACs to various of the Zeitlin Entities, rather than one entity. Likewise, publicly available FEC reports for PACs that used the Zeitlin Call Centers listed PAC payments made to multiple Zeitlin Entities rather than to one entity, and the PACs therefore appeared to pay different business rather than one business. In addition, ZEITLIN directed an employee to create fraudulent invoices billing certain PACs at an hourly or per-unit rate when, in truth and in fact, each entity was paid not by the hour, but rather, as part of ZEITLIN's overall collection of a large percentage of the money raised (typically approximately 90 percent).

c. On or about December 8, 2020, while testifying under oath during a deposition in connection with a federal civil matter, ZEITLIN falsely stated, in substance and in

part, that neither he nor employees of the Zeitlin Entities provided input as to the call scripts used by the Zeitlin Call Centers when making telemarketing calls on behalf of PACs. In truth and in fact, ZEITLIN and the employees of the Zeitlin Call Centers frequently provided input on and changed call scripts, including by adding false and misleading statements into the call scripts.

d. On or about March 31, 2022, in a declaration filed under penalty of perjury to a federal judge, ZEITLIN falsely stated that, among other things, he was not associated with and did not direct, supervise, or control certain of the New Zeitlin Entities. In truth and in fact, ZEITLIN controlled all the New Zeitlin Entities throughout their existence by exercising ultimate authority over managerial, operational, and financial decisions, including at the time he signed this declaration.

ZEITLIN'S ORDER TO DESTROY RECORDS

14. Beginning in or about 2018 to the present, RICHARD ZEITLIN, the defendant, has maintained a practice of principally communicating with employees of the Zeitlin Call Centers by phone or by encrypted messaging applications that typically delete data after a specified time period, or communicating with employees indirectly through an intermediary. For example, in or about 2018, ZEITLIN, directed certain employees of the Zeitlin Entities to delete materials and documents bearing ZEITLIN's name. In addition, ZEITLIN regularly received information about the operations of the business from CC-1 and relayed messages to others through CC-1.

15. On or about May 24, 2022, in connection with a federal investigation, law enforcement officers served federal grand jury subpoenas to certain individuals associated with the Zeitlin Entities and the PACs for which they solicited donations. On or about the same date, RICHARD ZEITLIN, the defendant, learned about the federal subpoenas and instructed CC-1 to delete his communications on a particularly electronic messaging application ("Application-1")

that Zeitlin's employees used internally to communicate with one another. ZEITLIN also instructed CC-1 to direct other of Zeitlin's employees to do the same. CC-1 relayed ZEITLIN's instruction to certain of Zeitlin's employees. The electronic messages that ZEITLIN instructed his employees to destroy contained internal communications among Zeitlin's employees about the Zeitlin Call Centers and the operations of the Zeitlin Entities, among other things.

STATUTORY ALLEGATIONS

COUNT ONE
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

16. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

17. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343, and did engage in the foregoing in connection with the conduct of telemarketing.

18. It was a part and an object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, ZEITLIN agreed with one or more others to engage in a scheme

to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1349 and 2326.)

COUNT TWO
(Wire Fraud)

The Grand Jury further charges:

19. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

20. From at least in or about 2017 through at least in or about 2020, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, in connection with the conduct of telemarketing, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, ZEITLIN engaged in a scheme to defraud donors of certain PACs through false and misleading statements, made during telemarketing calls soliciting donations, about what donations to the PACs would be used for and the nature of the PACs, and sent and received, and caused others to send and receive, wire communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1343, 2326, and 2.)

COUNT THREE
(Conspiracy to Obstruct Justice)

The Grand Jury further charges:

21. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

22. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to obstruct justice, in violation of Title 18, United States Code, Section 1512(c).

23. It was a part and object of the conspiracy that RICHARD ZEITLIN, the defendant, and others known and unknown, would and did corruptly alter, destroy, mutilate, and conceal a record, document, and other object, and attempt to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise would and did corruptly obstruct, influence, and impede an official proceeding, and attempt to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Section 1512(c) and (k).)

COUNT FOUR
(Obstruction of Justice)

The Grand Jury further charges:

24. The allegations set forth in paragraphs One through Fifteen are incorporated by reference as if set forth fully herein.

25. In or about May 2022, in the Southern District of New York and elsewhere, RICHARD ZEITLIN, the defendant, corruptly altered, destroyed, mutilated, and concealed a record, document, and other object, and attempted to do so, with the intent to impair the object's integrity and availability for use in an official proceeding, and otherwise corruptly obstructed, influenced, and impeded an official proceeding, and attempted to do so, to wit, after learning that federal grand jury subpoenas had been issued by a federal grand jury in the Southern District of New York that requested certain records of ZEITLIN's businesses, among other things, ZEITLIN instructed CC-1 to delete certain electronic messages and to direct employees of the Zeitlin Entities to delete certain electronic messages.

(Title 18, United States Code, Sections 1512(c) and 2.)

FORFEITURE ALLEGATION

26. As a result of committing the offenses alleged in Counts One and Two of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(8) and 2328, any and all real or personal property used or intended to be used to commit, to facilitate, or to promote the commission of said offenses; and any and all real or personal property constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of said offenses including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses, and any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offenses.

27. As a result of committing the offenses alleged in Counts Three and Four of this Indictment, RICHARD ZEITLIN, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28 United States Code, Section 2461(c),

any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

28. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982 and 2328;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

FOREPERSON

DAMIAN WILLIAMS
United States Attorney

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
1835 EAST CHARLESTON BOULEVARD, LAS VEGAS, NEVADA 89104

Case No. 2:23-MJ- 743 -VCF

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Nevada
(identify the person or describe the property to be searched and give its location):

See Attachment A-2

I hereby attest and certify on 8/16/23 that the foregoing document is a full true and correct copy of the original on file in my office, and in my legal custody.

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA
BY: _____ Deputy
Secretary

The search and seizure are related to violation(s) of *(insert statutory citations)*:

(1) 18 U.S.C. §§ 1349 and 2326 (conspiracy to commit wire fraud); (2) 18 U.S.C. §§ 1343, 2326, and 2 (wire fraud); (3) 18 U.S.C. § 1512(c), (k) (conspiracy to obstruct justice); and (4) 18 U.S.C. § 1512(c) (obstruction of justice)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-2

YOU ARE COMMANDED to execute this warrant on or before 22 LC August ~~30~~, 2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/16/23 11:30AM

CAM FERENBACH
Judge's signature

City and state: Las Vegas, Nevada

Hon. Cam Ferenbach
Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is 1835 East Charleston Boulevard, in Las Vegas, Clark County, Nevada 89149 ("Subject Premises-2"), particularly described as a commercial property with a reddish-brown brick exterior, windows with white window frames, and a flat white awning that reads "CHARLESTON PROFESSIONAL BUILDING" in dark blue print on the left and "GENERAL CONTRACTOR" in lighter blue print on the right when facing Subject Premises-2. A white rectangular placard with the numbers "1835" in white sits above the white awning and is affixed to a white architectural structure with columns and grating. In front of Subject Premises-2 are approximately six parking spaces for vehicles to park perpendicular to the street in front of Subject Premises-2. The door to Subject Premises-2 is white and below and offset to the left of the portion of the awning that reads "GENERAL CONTRACTOR."

Two images of Subject Premises-2 are below with the white door highlighted with a red circle in the second image below. Subject Premises-2 does not include the orange building depicted in the images below that is to the right of Subject Premises-2 and marked with a placard reflecting a street number of "1837."


1900 E Charleston Blvd
WE FIX PHONES
FOR LEASE
BUILD TO SUIT
3B7 PHONE HOUSE
CHARLESTON PROFESSIONAL BUILDING
GENERAL CONTRACTOR
LIQUIDATION
Google


Las Vegas, Nevada
FOR EASE
IMMEDIAT OCCUPANC
UTILITIES INCLUDED
NO CAMS
BUILD TO SUIT
702 278 1275
CHARLESTON
BUILDING
GEN RAL CONTRACTOR
1837
Google

ATTACHMENT B-2

PROPERTY TO BE SEIZED FROM SUBJECT PREMISES-2

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, of violations of 18 U.S.C. §§ 1349 and 2326 (wire fraud conspiracy and attempt), §§ 1343, 2326, and 2 (wire fraud and attempt to commit wire fraud), and § 1512(c) & (k) (obstruction of justice and conspiracy to obstruct justice) (together, the "Subject Offenses"), described as follows:

a. Evidence concerning occupancy or ownership of Subject Premises-2, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

b. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

c. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Richard Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

d. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

e. Materials relating to call centers associated with and/or operated by Zeitlin and their operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

f. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the

"Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

g. Evidence of the nature and development of the relationships among co-conspirators and witnesses, including but not communications, limited to social connections, prior business dealings, personal relationships, financial compensation, and loans.

h. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

i. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACS, including communications.

j. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

k. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

l. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

m. Evidence of call center policies and/or regulations.

n. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

o. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

p. Evidence of efforts to use and use of encrypted applications, programs, and devices.

q. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

r. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

s. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.

t. Evidence reflecting or relating to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence.

u. Any and all electronic devices, as defined below, used by or that appears to have been used by Zeitlin and current and former employees and/or associates of Zeitlin, and/or in connection with call centers and/or entities associated with and/or operated with Zeitlin.

v. A black and silver computer monitor and computer tower that is believed to have been used by and/or appears to have been used by a former employee of Zeitlin.

w. Evidence of the ownership, use, or control of the seized electronic devices.

2. As used herein, the term "electronic device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central-processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as USB flash drives, hard disk drives, compact disks, and other magnetic or optical media, and memory chips; and security devices.

3. This warrant authorizes a review of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to identify the user of the electronic device and/or whether or not the electronic device should be seized, copied, or returned. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means ☑ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Twenty-Nine Electronic Devices Seized in Las Vegas, Nevada, on or about August 17, 2023, USAO No. 2018R01129	)	**23 MAG 6429** Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

The search and seizure are related to violation(s) of *(insert statutory citations)*:

18 U.S.C. §§ 1349 and 2326 (conspiracy to commit wire fraud); 18 U.S.C. §§ 1343, 2326, and 2 (wire fraud); 18 U.S.C. § 1512(c), (k) (conspiracy to obstruct justice); and 18 U.S.C. §§ 1512(c) and 2 (obstruction of justice)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A.

YOU ARE COMMANDED to execute this warrant on or before September 29, 2023 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Duty U.S.M.J. .

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 09/15/2023 3:53pm

Sarah Cave

Judge's signature

City and state: New York, New York

The Hon. Sarah L. Cave, U.S.M.J.

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Devices Subject to Search and Seizure

The devices that are the subject of this search and seizure warrant (the "Subject Devices") are described as follows and presently located in the Southern District of New York:

Subject Device	Description	FBI Item No.	Seizure Premises[6]
1	Grey Apple iPad tablet with black keyboard case, Model A2378, S/N T045J4W21D	1B17	Zeitlin Premises-1
2	Apple iMac computer, Model A1419, S/N C02X61YWJ1GH	1B18	Zeitlin Premises-1
3	Apple iPad tablet, Model A1822, S/N DMPZKKJJHLF9	1B23	Zeitlin Premises-1
4	Samsung Galaxy Note 9 cellphone, Model SM-N6904, IMEI 351884708468626	1B25	Zeitlin Premises-1
5	White and gold Apple iPhone cellphone, IMEI 351884708468626	1B26	Zeitlin Premises-1
6	Apple iPad tablet, Model A1822, S/N DMPVKJTAHLF9	1B32	Zeitlin Premises-1
7	Samsung cellphone, Model SM-S908VZWFXAA, IMEI 357111203204742	1B34	Zeitlin Premises-1
8	Apple iPhone cellphone, Model A2651, S/N CXRTWW4P6K	1B35	Zeitlin Premises-1
9	Apple MacBook Pro laptop computer, Model A1502, S/N C02RG06DFVH9	1B36	Zeitlin Premises-1
10	Apple iMac computer, Model A2115, S/N H12DFHJLPN77	1B39	Zeitlin Premises-1
11	Grey Apple MacBook Pro, Model A2141, S/N C02FC6H1M-D6N	1B16	Zeitlin Premises-1
12	Silver Samsung cellphone with case, IMEI 351381563505451	1B15	Zeitlin Premises-1
13	Desktop Computer, Service Tag D33DHX1	1B46	Zeitlin Premises-2
14	Desktop Computer, Service Tag D36DHX1	1B47	Zeitlin Premises-2
15	Desktop Computer, Service Tag D2XCHX1	1B48	Zeitlin Premises-2
16	Dell Chromebook Computer, Serial Tag 6DNZ28B2	1B49	Zeitlin Premises-2
17	Desktop Tower with Post-It Note and "ENERMAX" case	1B50	Zeitlin Premises-2
18	Desktop Computer, Service Tag D33BHX1	1B51	Zeitlin Premises-2
19	Desktop Computer, Service Tag D30CHX1	1B52	Zeitlin Premises-2

[6] Zeitlin Premises-1 is the property located at 7815 West La Madre Way, Las Vegas Nevada 89149, and Zeitlin Premises-2 is the property located at 1835 East Charleston Boulevard, Las Vegas, Nevada 89104.

2022.01.31

20	Desktop Computer, Service Tag D34DHX1	1B53	Zeitlin Premises-2
21	Desktop Computer GGPPK02	1B54	Zeitlin Premises-2
22	Hard Drive	1B74	Zeitlin Premises-2
23	Hard Drive, S/N WX20C7979315	1B75	Zeitlin Premises-2
24	Kensington USB Drive 17009	1B78	Zeitlin Premises-2
25	Phone with call number 702-278-1275	1B79	Zeitlin Premises-2
26	SanDisk USB drive	1B80	Zeitlin Premises-2
27	Hard Drive, S/N 11500325584F	1B81	Zeitlin Premises-2
28	Desktop Computer, Service Tag D35DHX1	1B88	Zeitlin Premises-2
29	Dell Optiplex 3010 Desktop Computer, Service Tag D2ZDHX1	1B87	Zeitlin Premises-2

II. Review of ESI on the Subject Devices

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1349 and 2326 (conspiracy to commit wire fraud); 18 U.S.C. §§ 1343, 2326, and 2 (wire fraud); 18 U.S.C. § 1512(c), (k) (conspiracy to obstruct justice); and 18 U.S.C. §§ 1512(c) and 2 (obstruction of justice) (the "Subject Offenses") described as follows:

1. Materials, including documents, records, and communications reflecting the control, ownership, and management of businesses and entities associated with Richard Zeitlin, including but not limited to call center, telemarketing, IT, payroll, data, and real estate businesses such as: MRZ Management, Chrome Builders Construction, Courtesy Call, Donor Relations, Unified Data Services, a/k/a "Cloud Data Services," Compliance Consultants, a/k/a "American PCI," American Technology Services, a/k/a "Unlimited Technical Support," TPFE, Advanced Telephony Consultants, a/k/a "Advanced TCI," a/k/a "ATC," Cloud Data Services, LAV Services, EYP Consultants, Wired4Data, and Standard Data Services.

2. Materials, including documents, records, and communications, concerning potential, former, and current clients of call centers associated with and/or operated by Richard Zeitlin, including political action committees ("PACs") and charities, and their owners, treasurers, boards, and employees.

3. Evidence of contracts or agreements between any entities or businesses associated with call centers associated with and/or operated by Zeitlin, and their clients, contractors, and employees, including communications.

4. Materials relating to call centers associated with and/or operated by Zeitlin and their operations, and communications about Zeitlin's call center business and its operations, including call scripts, call recordings, sound recordings, mailers, donor lists, call lists, potential donor lists, contracts, invoices to clients, employee identities and locations, budgets, profit and loss statements, documents of incorporation, ownership, and organizational structure.

5. Materials concerning the identities and roles of those who have committed the Subject Offenses (the "Subjects") and the victims of the Subject Offenses (the "Victims"), and communications with and among Subjects, Victims, and potential witnesses to the Subject Offenses.

6. Evidence of the nature and development of the relationships among co-conspirators and witnesses, including but not communications, limited to social connections, prior business dealings, personal relationships, financial compensation, and loans.

7. Materials reflecting or relating to an agreement to engage in fraud, such as communications constituting, or discussing or regarding, making misleading or false representations to potential donors.

8. Materials reflecting or relating to making false and/or misleading statements to auditors, investors, regulators, investigating agencies, the judiciary, law enforcement, clients, employees, and potential donors and/or donors to charities and/or PACs, including communications.

9. Evidence of complaints about call centers, donor solicitations, and/or mailers associated with and/or operated by Zeitlin.

10. Evidence of complaints about clients or potential clients of call centers associated with and/or operated by Zeitlin.

11. Materials relating to regulations, rules, and state and federal laws, for telemarketers, call centers, solicitations, charities, PACs, and financial transfers.

12. Evidence of call center policies and/or regulations.

13. Materials reflecting or relating to the assets, income, liabilities, and/or expenditures of Richard Zeitlin and the Subjects, including financial statements, bank records, loan documents, and wire transfer records.

14. Evidence of motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations, regardless of time frame, and profits and/or losses.

15. Evidence of efforts to use and use of encrypted applications, programs, and devices.

16. Evidence relating to efforts to conceal the Subject Offenses and evade law enforcement and/or regulatory agencies.

17. Evidence of efforts to destroy evidence of the Subject Offenses and/or directions to others to do the same.

18. Evidence of the deletion and/or destruction of evidence of the Subject Offenses.